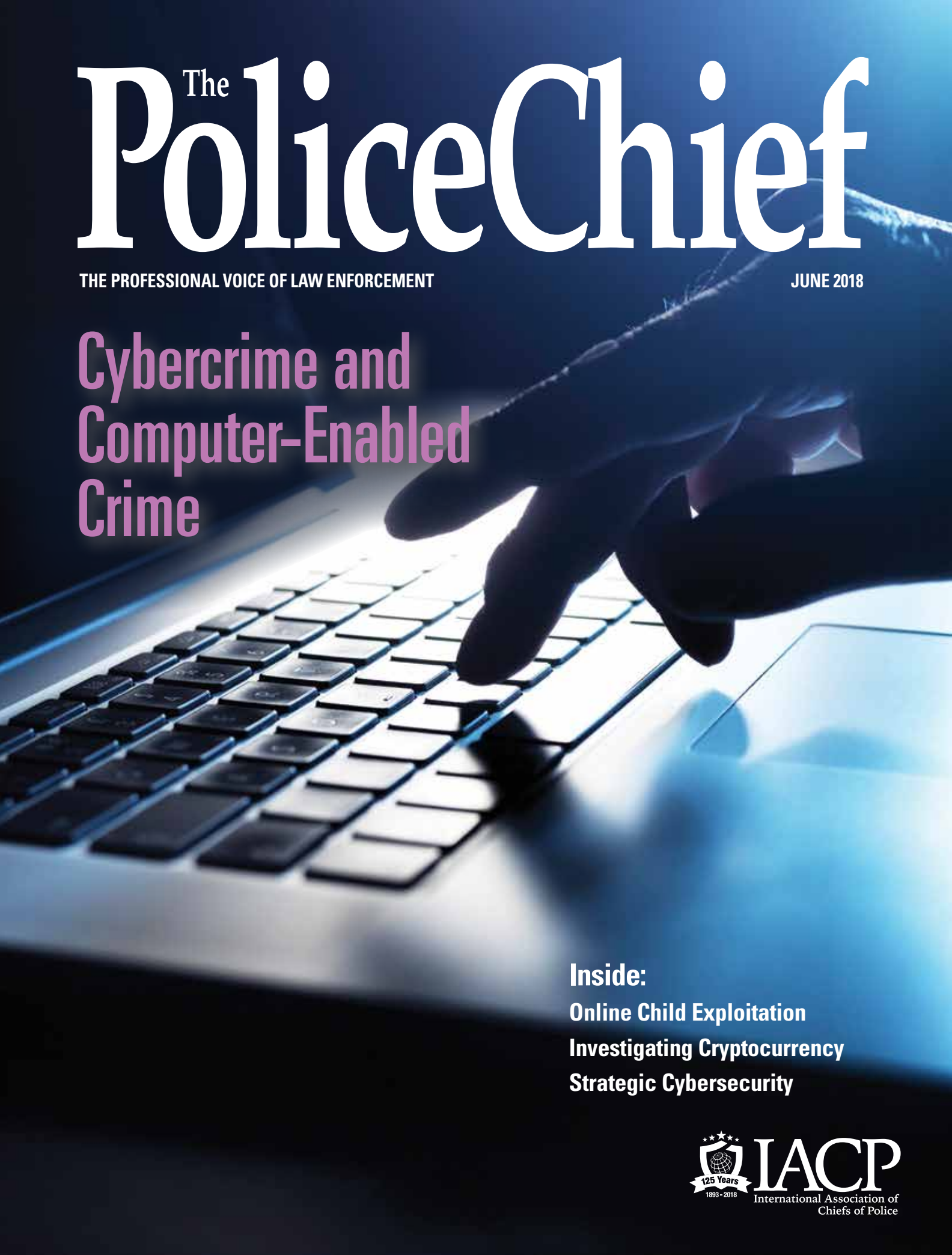
The PoliceChief

THE PROFESSIONAL VOICE OF LAW ENFORCEMENT

JUNE 2018

Cybercrime and Computer-Enabled Crime



Inside:

Online Child Exploitation

Investigating Cryptocurrency

Strategic Cybersecurity

125 Years 1893-2018

IACP International Association of Chiefs of Police

ASIS INTERNATIONAL
Advancing Security Worldwide®

REACH NEW HEIGHTS
GET CERTIFIED

SUCCESSFUL LAW ENFORCEMENT PROFESSIONALS DON'T STAND STILL...AND NEITHER CAN YOU.

Globally recognized as a mark of excellence in security management, ASIS board certification can help you succeed now—and in a second career. Transferable across all industry sectors and geographic borders, earning the CPP, PCI, or PSP eases your transition to the private sector.

CPP® PCI® PSP®

"I see the CPP as a benchmark and seal of approval. I'm recognized as a subject matter expert, and I've been given greater job responsibilities."

Nicholas G. Breiner, CPP, PCI, PSP,
Police Captain, Belleville Police Department

Isn't it time you get certified?

asisonline.org/pcm

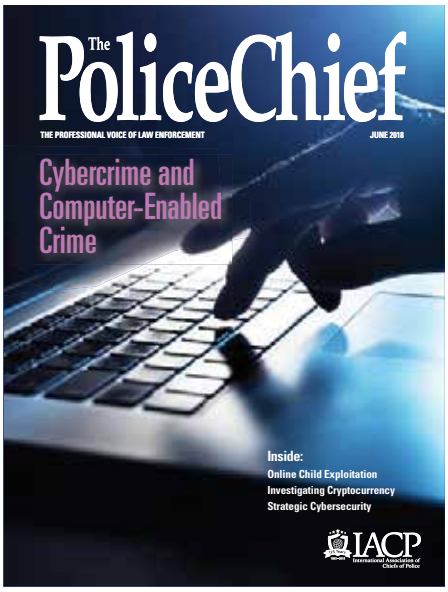
UN-CAR
YOUR IN-CAR

Introducing the new Axon Fleet 2

There are lots of in-car systems out there. But there's only one un-car system—technology that extends beyond the actual vehicle to integrate your body cameras, evidence and CEWs. Take advantage of night vision, easy installation and more for just $129/month. For more information: **www.axon.com/fleet2**

AXON, Axon and Axon Fleet 2 are trademarks of Axon Enterprise, Inc., some of which are registered in the US and other countries. For more information, visit www.axon.com/legal. All rights reserved. © 2017 Axon Enterprise, Inc.

AXON



With the rise in Internet accessibility and the commonality of Internet-enabled devices, it is inevitable that policing in the 21st century involves investigating and combating cybercrime and computer-enabled crime. While the goals are the same as in all crime prevention—protecting members of the global community, halting criminals before they offend again, and promoting overall public safety and quality of life—fighting cyber and computer crimes comes with additional challenges, including constantly evolving technology, digital evidence, multi-jurisdictional (and global) collaboration, and securing crucial data.

The PoliceChief

JUNE 2018
VOLUME LXXXV, NUMBER 6

The official publication of the International Association of Chiefs of Police, Inc.

Gene Voegtlin/*Editor*
Danielle Gudakunst/*Managing Editor*
Eric Delaune, Meghann Casanova, and Mike Prado/*Guest Editors*
Margaret M. White/*Proofreader*
The Townsend Group/*Advertising*
Christian D. Faulkner and Mara Johnston/*Member Services*
TGD Communications, Alexandria,Virginia/*Graphic Design and Production*
Amanda Burstein, Sam Capogrossi, Michael Fergus, Sarah Guy, Domingo Herraiz, Sarah R. Horn, Kathleen Kelley, Karen Maline, Rebecca Simonelli, Lynne Goto Uyema, Erin Vermilye/*Editorial Advisors*
Howe & Hutton, Ltd./*Legal Counsel*

http://www.policechiefmagazine.org

© Copyright 2018, by the International Association of Chiefs of Police, Inc. Reproduction of any part of this magazine without express written permission is strictly prohibited.

The Police Chief (ISSN 0032-2571) is published monthly by the International Association of Chiefs of Police, 44 Canal Center Plaza, Suite 200, Alexandria, VA 22314-2357, USA; 703-836-6767; fax: 703-836-4543. Periodicals postage paid at Alexandria, Virginia, and additional mailing offices. Subscription rate of $30 to IACP members is included in annual membership dues; subscription rate to nonmembers is $30 per year, domestic and foreign. Single copy, current issue, $2.50; back issues, $3, except APRIL Buyers' Guide issue, $12.50.

POSTMASTER: Send address changes to the *Police Chief*, 44 Canal Center Plaza, Suite 200, Alexandria, VA 22314, USA.

Canada Post: Publications Mail Agreement #40612608
Canada returns to be sent to Bleuchip International, P.O. Box 25542, London, ON N6C 6B2

NOTE: New subscriptions and changes of address require six to eight weeks to process. Subscriptions begin with next available issue; for backdated subscriptions, place separate order for back issues desired. IACP will not be responsible for replacement of an issue if not notified of nondelivery by the 15th of the third month following the month of issue. Please check address label and promptly mail any necessary changes.

Articles are contributed by practitioners in law enforcement or related fields. Manuscripts must be original work, previously unpublished and not simultaneously submitted to another publisher. No word rate is paid or other remuneration given. ***Contributors' opinions and statements are not purported to define official IACP policy or imply IACP endorsement.***

Printed in the USA.

BPA business publication membership granted September 1991

ARTICLES

24 Protecting the Powerless: Combating Cyber Child Sexual Exploitation
By John F. Clark

28 Following the Money: Investigating Cryptocurrency
By John Hedrick and Jeremy Bluto

30 Cybersecurity Leadership for Today's Law Enforcement Executive: Two Strategic Issues
By Pedro D. Cordero

38 Myths and Realities of Going Dark: Talking Points for SLTT LE Executives
By Rich Littlehale, Thomas Ruocco, and Jim Emerson

42 Starting a Forensic Video Unit: What Chiefs Need to Know
By Brandon Epstein

50 The FBI's NIBRS Transition: Questions and Answers
By Jeffrey Fisher

54 Race to the Cloud... Proceed with Caution
By Scott A. Vantrease, Jim Emerson, and Eldon Amoroso

IACP THROUGH THE YEARS:

1999

60 The Evolution of the Computer Hacker's Motives
By Matthias A. Joyce and Shawn Barrett

74 Today's Police Chiefs' Greatest Challenge Accountability, Accountability, Accountability!
By Hajir Nuriddin

COLUMNS

6 President's Message: Equipping for the Reality We Face: Addressing Community and Media Backlash
By Louis M. Dekmar

10 Legislative Alert: IACP Advocates Creating a National Commission on Criminal Justice
By Sarah Guy

12 Officer Safety Corner: Fatigue Management Training
By Lois James and Fiona Vincent

18 Research in Brief: Officer-Involved Shootings: Context Means Everything
By Justin Nix and Geoffrey Alpert

20 Chief's Counsel: Life After *Liverman*: Continuing to Police Employee Speech on Social Media
By Eric R. Atstupenas

46 Product Feature: Getting the Details Right Is Key for Safety Gear
By Scott Harris

76 Technology Talk: New Technology and Funding Opportunities
By Domingo Herraiz

78 Traffic Safety Initiatives: Crash Reporting Centers: Moving Crash Reporting Away from the Roadway
By Howard B. Hall

80 IACP Working for You: IACP 23rd Annual Training Conference on Drugs, Alcohol, and Impaired Driving
By Chuck Hayes

DEPARTMENTS

8 The Dispatch

66 New Members

69 Line of Duty Deaths

70 Product Update

82 Index to Advertisers

BPA WORLDWIDE

VISIT POLICE CHIEF ONLINE
www.policechiefmagazine.org
to read online-only bonus articles! A new article is posted each week.

ASSOCIATION OFFICERS — 2017–2018

Immediate Past President Donald W. De Lucca, Chief of Police, Doral Police Department, 6100 NW 99 Avenue, Doral, FL 33178

President Louis M. Dekmar, Chief of Police, LaGrange Police Department, 100 W Haralson St, LaGrange, GA 30241

First Vice President Paul Cell, Chief of Police, Montclair State University Police, College Avenue, Montclair, NJ 07043

Second Vice President Steven Casstevens, Chief of Police, Buffalo Grove Police Department, 46 Raupp Blvd, Buffalo Grove, IL 60089

Third Vice President Cynthia Renaud, Chief of Police, Santa Monica Police Department, 333 Olympic Drive, Santa Monica, CA 90401

Fourth Vice President Dwight Henninger, Chief of Police, Vail Police Department, 75 S Frontage Rd, Vail, CO 81657

Vice President at Large Richard E. Smith, Chief of Police, Wakefield Police Department, 1 Union Street, Wakefield, MA 01880

Vice President at Large Wade Carpenter, Chief of Police, Park City Police Department, 2060 Park Avenue, Park City, Utah 84060

Vice President–Treasurer Ken Walker, Chief of Police, West University Place Police Department, 3800 Boulevard, West University Place, TX 77005

Division of State Associations of Chiefs of Police General Chair Timothy Lowery, Chief of Police, Florissant Police Department, 1700 N Hwy 67, Florissant, MO 63033

Division of State and Provincial Police General Chair Tracy Trott, Colonel, Tennessee Highway Patrol, 1150 Foster Avenue, Nashville, TN 37243

Division of Midsize Agencies General Chair David Rausch, Chief of Police, Knoxville Police Department, 800 Howard Baker Jr. Avenue, Knoxville, TN 37915

Parliamentarian Michael Caldwell, General Counsel, Georgia Association of Chiefs of Police, 3500 Duluth Park Lane, Suite 700, Duluth, GA 30096

Executive Director and Chief Executive Officer Vincent Talucci, International Association of Chiefs of Police, 44 Canal Center Plaza, Suite 200, Alexandria, VA 22314

Deputy Executive Director and Chief Operating Officer Terrence M. Cunningham, International Association of Chiefs of Police, 44 Canal Center Plaza, Suite 200, Alexandria, VA 22314

IACP Fellows

David Becker, United States Army

Kimberly Burrus, Baltimore, Maryland, Police Department

Thomas Coghlan, New York City Police Department

Eric Delaune, U.S. Homeland Security Investigations

Shahram Fard, Alexandria City, Virginia, Police Department

Nancy Jackson, Prince George's County, Maryland, Police Department

Tasha Wilcox, U.S. Customs and Border Protection

Annual IACP Conferences

2018 (125th) • Oct. 6–9 • Orlando, FL

2019 (126th) • Oct. 26–29 • Chicago, IL

2020 (127th) • Oct. 17–20 • New Orleans, LA

Ensuring Integrity. Worldwide.

Over 750 public safety agencies in the United States, Australia, Canada and New Zealand stake their reputations on IAPro.

They know that detecting performance and misconduct issues upstream before they become serious is a best practice they can't afford to be without.

To learn more about IAPro and proactive integrity, contact us at 800-620-8504 or www.iapro.com.

IAPRO

THE LEADING PROFESSIONAL STANDARDS SOFTWARE. WORLDWIDE.

www.iapro.com

STICKERS FOR KIDS

with your department's name and state's official seal

Junior Officer Badge Stickers
Safety Message Stickers
Star Shaped Badge Stickers

Visit Our Website at:
www.PoliceStickers.com
Phone: 508-892-1555 Email: sales@policestickers.com

Equipping for the Reality We Face: Addressing Community and Media Backlash

Although some of the rhetoric around the "militarization of police" has quieted down, I still catch rumblings, observe media coverage, and hear from our members that they cannot seem to shake the contrived image that has been unfairly cast over the profession.

For me, it seems to be pretty clear—when law enforcement is dealing with fleeing suspects, active shooters, or terrorists, why wouldn't there be an expectation that the police are adequately equipped to safeguard the public? A police officer on foot or in their cruiser is agonizingly vulnerable, even when they are wearing their vests and armed, and, if we leave officers vulnerable and unmatched for criminals, they will not be able to protect the members of their communities or themselves.

When responding to events—vehicle or knife attacks, bombs, active shooters, the pursuit of a lone suspect or multiple suspects—our officers need to be properly equipped and prepared to meet any number of life-threatening situations. The critical incidents in Paris, France; San Bernardino, California; the Pulse nightclub in Orlando, Florida; and Las Vegas, Nevada were all instances where it was absolutely necessary for the police to be properly armed and equipped to quickly end the attacks and safeguard the public.

There are countless other incidents that go back in history, like the North Hollywood bank robbery that occurred over two decades ago, where 1,100 rounds of armor-piercing bullets were fired by two suspects. A SWAT team and specialized equipment were necessary to resolve the situation, but only after 11 police officers and 7 civilians were injured.

However, these few examples are only a handful of the high-profile incidents that have grabbed the world's attention in news headlines. Some specific events may have contributed to the inaccurate perception of today's police as a hardened militarized force, rather than selfless officers who would give their lives to protect their communities. Although the need for police to have the proper equipment seems clear, there are still individuals and organizations who do not think our officers should have use of helmets, shields, patrol rifles, batons, armored vehicles, or tear gas.

Every second of every day while on duty, we have an obligation to be staffed and equipped for any life-threatening episode… the safety of our communities and our officers require no less.

What I would ask those that would oppose properly equipping our officers is this: "If you were a hostage trapped in the Pulse nightclub or attending the concert at the Bata clan concert hall in Paris, hiding as gunmen fired into the crowd, would you not expect men and women of law enforcement to enter that building and be properly equipped to defend against or stop the criminals they face?"

Every year, millions of people are treated in hospital emergency rooms across the world. A fraction of those encounters are immediately life threatening. Nonetheless, each emergency room is staffed and equipped for any potential life-threatening episode; no one would expect differently. The reality is that a large part of what police officers do does not involve facing down criminals, but rather serving the members of our communities. However, every second of every day while on duty, we have an obligation to be staffed and equipped for any life-threatening episode… the safety of our communities and our officers require no less. ❖

Louis M. Dekmar, Chief of Police, LaGrange, Georgia, Police Department

FURTHER READING

Agencies use the equipment available in innovative and inspiring ways to serve their communities to the best of their capabilities. To learn how one agency used an armored vehicle to save lives in its community during a natural disaster, visit Police Chief Online at www.policechiefmagazine.org/using-armored-vehicles-for-emergency-rescues.

ILLEGAL WINDOW TINT

What are they hiding ...
DRUGS? DUI? WEAPONS?

ENFORCER II TINT METER

$49.95 Law Enforcement Only Price

LASER LABS We Save Police Lives™

www.Laser-Labs.com

Over A Half Million Tint Meters Sold Since 1989

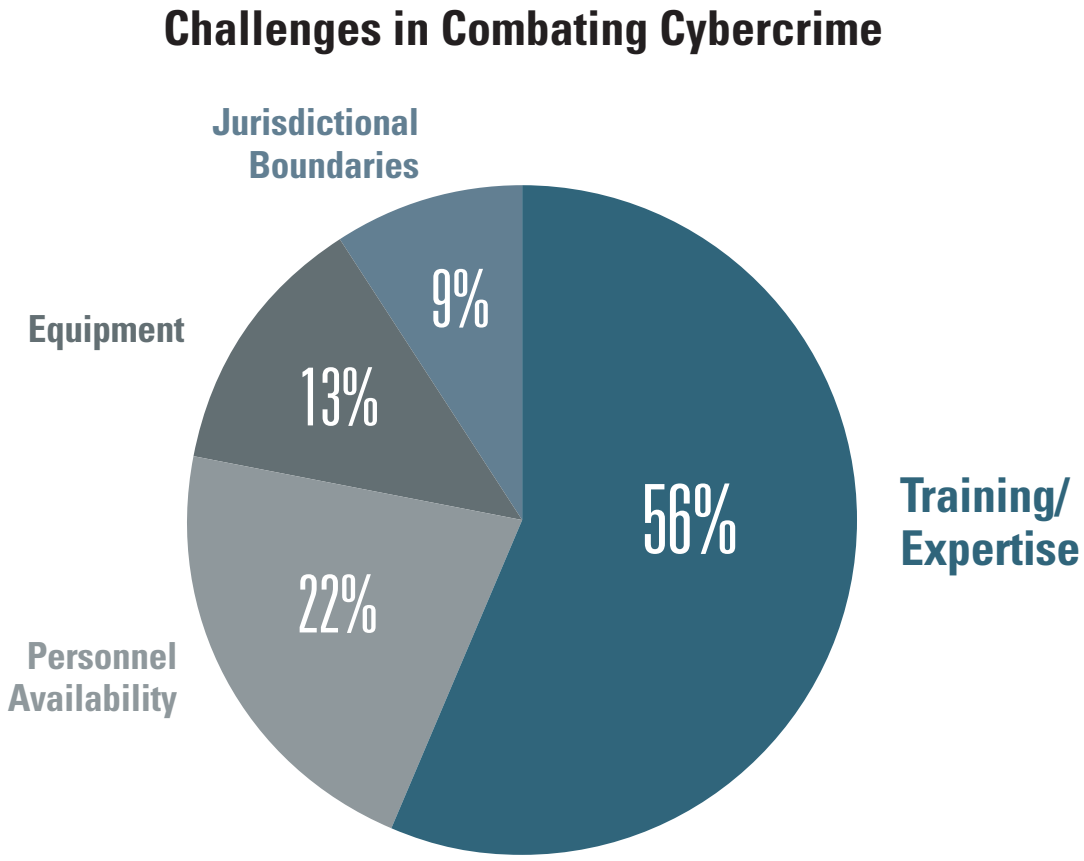
DESIGNED & ASSEMBLED IN U.S.A.

USA 800-452-2344 Email: Sales@Laser-Labs.com INT 1-781-826-4138

Police Chief *knows that many of the best ideas and insights come from IACP members who serve their communities every day. The Dispatch is an opportunity for members and other readers to share their wisdom, thoughts, and input on policing and the magazine.*

MEMBERS SPEAK OUT

In April, *Police Chief* asked to share their agencies' greatest challenges in combating cybercrime. Here's what you told us:



> "Our highest priority currently is filling the ranks to provide basic police services, leaving shortages in most specialty and proactive investigate units."
>
> —Gary Jones, Captain
> Yakima Police Department, Washington

"Because we are a small tribal department, we are often overlooked; thus, we do not have access to state or federal resources for training and tools."

—Edward Reina, Tribal Administrator
Reno-Sparks Indian Colony

"We have a very limited budget to purchase equipment needed to further digital forensics."

—Name withheld
Maryland

YOUR TURN

How has your agency increased its community policing efforts?

Visit **www.policechiefmagazine.org** to tell us your answer. Look for the results in the August 2018 issue of *Police Chief*!

Connect with IACP and *The Police Chief* on social media!

www.facebook.com/TheIACP

@IACP #PoliceChiefMag

http://theiacpblog.org

IACP DRUGS ALCOHOL & IMPAIRED DRIVING 2018
AUGUST 13-15
NASHVILLE
TENNESSEE
theIACP.org

Drug and alcohol abuse impacts communities around the world. **Are you equipped to navigate this evolving landscape?**

IACP International Association of Chiefs of Police

REGISTER NOW

for the **2018 IACP Annual Training Conference** on Drugs, Alcohol, and Impaired Driving and get the connections, strategies, and tools you and your agency need.

www.theIACP.org/DAIDconference

IACP Advocates Creating a National Commission on Criminal Justice

By Sarah Guy, Senior Advisor, IACP

For over two decades, the IACP's top legislative priority has been the creation of a National Commission on Criminal Justice. The last national commission, created in 1965 by U.S. President Lyndon Johnson, led to significant changes in the criminal justice system and put in place many lasting measures that fundamentally changed the way law enforcement agencies and the U.S. criminal justice system operated.

However, much has changed in criminal justice during the 50 years since the Johnson Commission, and the field is facing several important issues and challenges. These challenges are all interconnected and should not be handled in isolation from one another.

The establishment of a National Commission on Criminal Justice would not be just another government study; the establishment of such a commission would set forth a strategic blueprint for criminal justice that would guide U.S. law enforcement's efforts to protect communities for years to come.

The IACP has taken the following steps this month to advocate for a National Commission on Criminal Justice.

Chief Will Johnson Meets with Senator Cornyn and Jared Kushner. On May 11, 2018, IACP Board of Officers member Chief Will Johnson from the Arlington, Texas, Police Department met with Senate Majority Whip John Cornyn (R-TX) and U.S. President Trump's advisor Jared Kushner to discuss prison reform, specifically the FIRST STEP Act, a bipartisan measure aimed at lowering recidivism through rehabilitative programs at the federal level. The legislation is modeled after successful reforms that states like Texas, Georgia, and Rhode Island have implemented to rehabilitate low-risk offenders and prepare them to reenter society.

The legislation would direct the Bureau of Prisons (BOP) to conduct risk and needs assessments for each offender upon sentencing and offer individualized, evidence-based recidivism reduction plans to all inmates. Programs could include vocational training, educational support, substance abuse treatment, mental health care, anger management courses, faith-based initiatives, or other proven resources to lower the chance that individuals reoffend. BOP would continue to monitor individuals throughout this process to ensure the appropriate resources are being applied and successful reentry occurs.

The FIRST STEP Act would also prepare individuals to transition back into their communities by allowing them to serve the final days of their sentences in halfway houses or on home confinement.

During the meeting, Chief Johnson stressed the need for a national commission. The prison reform issue is a perfect example of how there is a desperate need for a system-wide approach in addressing criminal justice issues. True reform of the prison and corrections system will require changes to all aspects of the criminal justice system.

This approach also needs to include police officers and prosecutors, who need training, resources, and alternative options to ensure that those with mental illness are not being sent to jail instead of getting the medical services they need. Reform also requires efforts to ensure that individuals don't end up in prison in the first place. This means investing in a wide array of programs, from good educational systems and mentoring programs to initiatives targeting violent crime and drug rehabilitation programs.

Terrence Cunningham, IACP Deputy Executive Director, Testifies before the U.S. Commission on Civil Rights. On May 11, 2018, IACP Deputy Executive Director Terrence Cunningham testified before the U.S. Commission on Civil Rights at a hearing entitled *In the Name of Hate: Examining the Federal Government's Role in Preventing Hate Crimes.*

In his testimony, Deputy Executive Director Cunningham discussed the underreporting of hate crime statistics; the challenges law enforcement faces in investigating these specific crimes; and the impact of hate crimes on community-police relations. He also outlined actions the federal government can and should take to help improve response to hate crimes and to help prevent these heinous acts. The number one issue stressed was the need for Congress to pass the National Criminal Justice Commission Act (S. 573) to initiate a review of the criminal justice system at all levels and propose reforms to address the most pressing issues facing the U.S. criminal justice system, including hate crimes.

Other recommendations included designating federal program and funding assistance for enhanced training for law enforcement to identify, investigate, and report hate crimes; offering incentives, including additional financial resources through the Byrne JAG program, to states and localities to report hate crime data to the FBI; providing victim services assistance; and identifying funding to create specialized units and task forces to help agencies develop multiagency task forces.

IACP Meets with Senate Leadership. During National Police Week in May 2018, IACP leadership met with key U.S. senators to discuss issues such as officer safety and wellness and funding for key law enforcement grant programs. During the meeting, IACP also emphasized the importance of passing the National Criminal Justice Commission Act.

We hope that you will join the IACP in actively supporting our advocacy efforts for the establishment of a National Commission on Criminal Justice. For this to happen, your senators, representatives, and the administration needs to hear from you—their constituents and leaders in the law enforcement profession. It is imperative that they hear directly from the field about the need for a comprehensive review and report on the state of the criminal justice system in the United States. ❖

ACADIS®
READINESS SUITE
Create the
Ultimate
Training
Operation
Acadis connects every aspect of your training operation so it can intelligently communicate and accelerate tasks.
Start your creation at
info.acadis.com/ultimate
Software for public safety operations.
ENVISAGE
TECHNOLOGIES

Fatigue Management Training

By Lois James, PhD, Sleep and Performance Research Center, Washington State University, and Fiona Vincent, MSc, Manager, Fitness and Lifestyle Unit, Royal Canadian Mounted Police

It is becoming widely acknowledged that fatigue is a critical and pervasive problem in police personnel.[1] This recognition has been driven largely by research on the topic that shows police officers tend to be chronically fatigued and are therefore at a high risk for accident, injury, and error. For example, more than 90 percent of officers report being fatigued a majority of the time, and over a quarter of officers report falling asleep at the wheel within the past month.[2] Police fatigue is particularly concerning for night-shift officers, whose sleep is compromised by having to sleep during the day when their internal clock is pushing them to be awake, causing "circadian misalignment."[3]

Fatigue is not only associated with short-term risks; it is also associated with long-term health problems for police officers. For example, research looking at shift workers in general has found that shift work–related fatigue is associated with increased risk for cardiovascular, gastrointestinal, and metabolic diseases.[4] Police officers are more likely to suffer from these diseases than other workers, in addition to disproportionately suffering from sleep disorders, post-traumatic stress disorder, substance abuse disorder, and increased risk for suicide.[5]

In light of the extensive research suggesting that police officers are chronically fatigued and associating this fatigue with short- and long-term safety and wellness consequences, police executives are starting to search for potential solutions to reduce the impact of fatigue. One such strategy was employed by the Royal Canadian Mounted Police (RCMP) F Division (Saskatchewan) Fitness and Lifestyle Unit and was evaluated by a research team at Washington State University (WSU).

Methodology

Study Design

The RCMP fatigue training study was conducted over a 24-month period and involved an interdisciplinary and international partnership between the RCMP F Division's Fitness and Lifestyle Unit (the training team), the WSU Sleep and Performance Research Center (the evaluation team), and the Calgary-based Centre for Sleep and Human Performance (the clinical team). The study, and partnership was initiated by the Fitness and Lifestyle Unit, which recognized that fatigue was a serious concern to the RCMP and to the safety and health of its members. As such, they gathered a team to implement and evaluate a fatigue-management training strategy, the first of its kind within the policing profession.

Test Site and Participants

The RCMP is in the unusual position of serving national, federal, provincial, and municipal functions. It is the second largest police agency in North America (after the New York Police Department). The RCMP's F Division is made up of 133 detachments that police various geographical areas that can run up to an area of 20,000 sq km. The large geographical spread of F Division makes "on-call" duties unavoidable, during which members can return home to sleep but must be ready to return to work immediately when called.

A total of 165 members were recruited into the study. Of these, the majority (92 percent) were frontline operational "regular members." Participants represented both rural and urban detachments within the division. Study participants were mostly white (88 percent), male (70 percent), and married (61 percent). The average age of participants was 38 years with an average of 11 years of experience within the RCMP. Most participants worked rotating shifts (62 percent) and had on-call duties (58 percent). The shift lengths participants worked ranged from 8 to 12 hours, although all participants in the study had experienced working overtime. Only 5 percent of participants were additionally employed outside of the RCMP.

Training Intervention

The fatigue-training intervention implemented and evaluated in the current study was the Calgary Police Service (CPS) Fatigue Training Program, developed by Dr. Charles Samuels and gifted to the RCMP by CPS. The training is taught over three to four hours and covers the science of sleep, sleep disorders, and fatigue countermeasures. The current study used a train-the-trainer

CAPTURES 43,200 MOMENTS OF CLARITY

Capturing 12 hours of high-definition footage with just a single charge, the BWX-100™ body cam is ready to go the distance on every shift. Never miss a moment of action with our Bidirectional Triggering system and an easy-to-read, easy-to-use LCD display panel.

BWX100

ACTIONABLE INTELLIGENCE

bwx100.com

L3 Technologies

Mobile-Vision, Inc.

approach to deliver the intervention. Dr. Samuels taught members of the Fitness and Lifestyle Unit how to deliver the training effectively.

Test Measures

The baseline and post-training intervention assessment used in the current study was a survey including items on well-validated sleep health and wellness questionnaires.[6] Additional questions were also included from an internal RCMP Fitness and Lifestyle survey on physical activity and well-being. Altogether, these items were used to collect a broad snapshot of participant sleep, health, and wellness from multiple perspectives.

Participants were sent links to the survey by email, which they accessed via either a personal smartphone or mobile device or via their work computers. The survey was deployed both before and after the training. The link to the baseline assessment was sent immediately before training, and participants could not participate in the training until the survey was complete. The link to the post-training intervention assessment was sent four weeks after the training. Despite prompts, substantial study attrition was observed. Of the 165 participants who completed the training, only 77 completed the post-training intervention survey.

Key Results

Baseline

Analysis of baseline data revealed that on average, participants slept for just over six hours per night during their workweek and just under eight hours per night during their time off, which suggests they were likely to have been accumulating sleep debt over time. Even more alarming, almost three-quarters (70 percent) of the sample reported being routinely tired, almost half (45 percent) reported suffering from insomnia, and less than a quarter (21 percent) were satisfied with their sleep, indicating pervasive concerns about sleep and fatigue. Physical health was also a concern within the sample, with over half (51 percent) suffering from headaches and almost half (41 percent) reporting neck, back, or spine pain. Furthermore, mental health concerns were raised, with over half reporting feeling depressed (55 percent) or anxious (63 percent) on a regular basis.

Baseline to Post-Training Intervention Differences

When investigating changes from baseline to post-training intervention, it was revealed that participants experienced many positive sleep, health, and wellness benefits. The proportion of the sample suffering from insomnia dropped from 45 percent to 32 percent, the proportion satisfied with their sleep increased from 21 percent to 39 percent, and the proportion experiencing routine tiredness went from 70 percent to 60 percent. Regarding physical health, the proportion of the sample reporting suffering from headaches dropped from 51 percent to 27 percent and from neck, back, or spine pain dropped from 41 percent to 26 percent. Logistic regression models revealed that several of these differences pre- and post-training intervention were statistically significant, thus not likely to be due to chance.

Lessons Learned and Recommendations for Police

Management Support

For the fatigue intervention training to succeed, there is a critical need to have managerial and organizational endorsement of the project from the beginning.

- A champion at the senior management or executive level, who is able to consistently advocate the merits of the project and ensure its ongoing visibility is key to keeping the project on the managerial landscape.
- Financial funding will be needed to appropriately meet the project's needs and remain consistent throughout the duration of the project.
- The willingness of supervisors and frontline managers to endorse, allow, and encourage members to participate in the project is a major contributor to the project's viability.

Project Parameters

The scope, relevance, and parameters of the project need to be defined and adhered to. More specifically, the project leads should

- clearly identify the scope and intended outcomes of the project and how they relate to the organization's mandate and priorities, which is key to containing the project within its original parameters and encouraging managerial buy-in;
- recognize that the project might not be management's highest priority, yet tenaciously keep it in front of them by providing regular updates;
- bring in both external and internal experts who can attest to the relevance and importance of the project;
- establish a staged approach to the project that realistically meets the structure and bureaucracy of the organization; and
- communicate the milestones regularly to all stakeholders.

Overcoming Challenges

Observed challenges from the current study and tips for overcoming them include the following:

- Maintaining the interest and commitment of members over the course of the project presented challenges. The success of a fatigue management strategy depends upon members accepting that a healthy lifestyle, including adequate sleep, is a lifelong commitment that they will need to work at. Consider refresher or "booster" training, that can be condensed into five-minute modules, presented at roll call or distributed electronically to members.
- Both endorsement of the project from the top and interest in participating from the membership may evolve slowly and erratically. It is important to draw upon the curiosity of stakeholders to foster their initial participation and to sustain their interest over the duration of the project. Be patient—change takes time, but police health and wellness is worth investing in. ❖

The full study, "Evaluating the Effectiveness of Fatigue Management Training to Improve Police Sleep Health and Wellness: A Pilot Study" was published in the January 2018 issue of the *Journal of Occupational and Environmental Medicine.*

Notes:

[1]Bryan Vila, *Tired Cops: The Importance of Managing Police Fatigue* (Washington, DC: Police Executive Research Forum, 2000).

[2]Shantha M. W. Rajaratnam et al., "Sleep Disorders, Health, and Safety in Police Officers," *The Journal of the American Medical Association* 306, no. 23 (2011): 2567–2578.

[3]Bryan Vila, "Impact of Long Work Hours on Police Officers and the Communities They Serve," *American Journal of Industrial Medicine* 49, no. 11 (2006): 972–980.

[4]Stephen M. James et al., "Shift Work: Disrupted Circadian Rhythms and Sleep—Implications for Health and Well-being," *Current Sleep Medicine Reports* 3, no. 2 (2017): 104–112.

[5]John M. Violanti et al., "Life Expectancy in Police Officers: A Comparison with the U.S. General Population," *International Journal of Emergency Mental Health and Human Resilience* 15, no. 4 (2013): 217–228.

[6]Amy E. Bonomi et al., "Validation of the United States' Version of the World Health Organization Quality of Life (WHOQOL) Instrument," *Journal of Clinical Epidemiology* 53, no. 1 (2000): 1–12; Daniel J. Buysse et al., "The Pittsburgh Sleep Quality Index: A New Instrument for Psychiatric Practice and Research," *Psychiatry Research* 28, no. 2 (1989): 193–213; Craig S. Rosen et al., "Six and Ten Item Indices of Psychological Distress Based on the Symptom Checklist-90," *Assessment* 7, no 2 (2000): 103–111.

RESOURCE

IACP has produced a useful infographic on the effects of sleep deprivation. Visit www.theIACP.org/ICPRlawenforcementfamily for this and other wellness resources to share with your officers.

ADVANCED BY DESIGN.™ M&P®

INTRODUCING THE NEW M2.0™ COMPACT PISTOL SERIES.

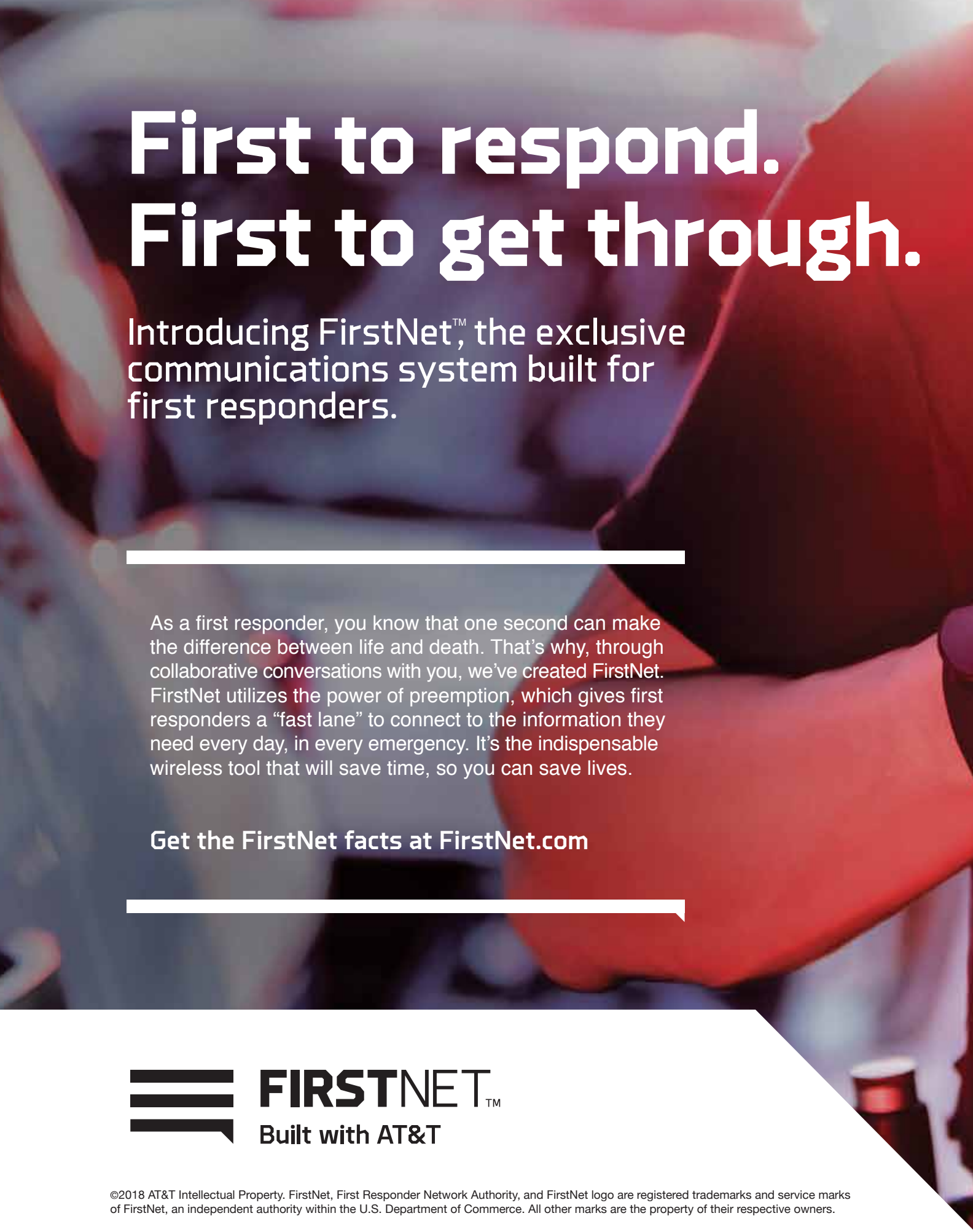
COMPACT CARRY ADVANTAGE: 4" BARREL, 15 ROUND MAGAZINE, M2.0™ FEATURE SET.

M2.0™

MADE IN USA

9MM -15RDS | 40S&W -13RDS

SMITH-WESSON.COM



First to respond. First to get through.

Introducing FirstNet™, the exclusive communications system built for first responders.

As a first responder, you know that one second can make the difference between life and death. That's why, through collaborative conversations with you, we've created FirstNet. FirstNet utilizes the power of preemption, which gives first responders a "fast lane" to connect to the information they need every day, in every emergency. It's the indispensable wireless tool that will save time, so you can save lives.

Get the FirstNet facts at FirstNet.com

FIRSTNET™
Built with AT&T

©2018 AT&T Intellectual Property. FirstNet, First Responder Network Authority, and FirstNet logo are registered trademarks and service marks of FirstNet, an independent authority within the U.S. Department of Commerce. All other marks are the property of their respective owners.

POLICE

Officer-Involved Shootings: Context Means Everything

By Justin Nix, Assistant Professor, University of Nebraska Omaha, and Geoffrey Alpert, Professor, University of South Carolina

Police use of deadly force is undeniably one of the most serious of all governmental acts. That said, this action is legally permissible in the United States in order to save a life, including that of an officer or innocent bystander. Until recently, it was not possible to determine the number of officer-involved shootings (OIS) that occur each year in the United States. Thanks to the *Washington Post*, three years of data now exist that show police fatally shoot approximately 1,000 people each year.[1] Other data sets have recently come into existence, including the OIS Data Collection Initiative by the Police Foundation and the Major Cities Chiefs Association (featured in the May 2018 *Police Chief*), as well as those by other media outlets and crowdsourced websites (e.g., *The Guardian*, killedbypolice.net, and fatalencounters.org).[2] These projects have generated data sets that suggest similar totals, with each data collection method having its particular strengths and limitations. While these data are critically important, they are limited to fatalities and provide no insight about "suicide-by-cop"; shootings that produce nonfatal injuries; misses; or situations in which officers could have fired a weapon but chose not to. Nevertheless, the data still provide a helpful numerator (total number of fatal police shootings) that was previously unknown. The challenge, then, is making sense of this numerator. In other words, what is the appropriate *denominator*?

Searching for an Appropriate Denominator

The denominator is the number against which the numerator is compared. This denominator issue has plagued police executives and researchers in a variety of areas. One of the most common is the concern of racial profiling in stops, searches, and arrests. Early research used the general population as the denominator, as it was easily available and made sense to those who did not consider at-risk subgroups of the population.[3] The problem, of course, is that using the general population as the denominator assumes all persons have an equal chance of interacting with police. Studies and police officers' experiences consistently conclude that this is not accurate.[4] Accordingly, the denominator should consist of the population at risk of being contacted by the police. After all, to be searched, arrested, or shot by police, one first must encounter an officer. Consider an example from another profession. In the study of maternal mortality rates, researchers use the number of maternal deaths as the numerator and the number of live births (rather than the population of all women) as the denominator, then multiply by 100,000. This calculation provides a rate that can be compared across jurisdictions and time.

Just as not all women will experience pregnancy, not all individuals of a specific population will encounter a police officer; therefore, one potential remedy concerning OIS is to use the number of people who are contacted by the police (including those who are field interviewed, ticketed, or arrested) as the denominator and use OIS incidents (whether fatalities, injuries, or shots fired) as the numerator. Arrests, for example, are available from the FBI's Uniform Crime Report (UCR). While this sounds like a good solution, the *Washington Post*'s data suggest many OIS fatalities involve non-criminal contacts—or, at least, civilian-police encounters where an arrest might not be expected. The *Washington Post* data show that between 2015 and 2017, just under 12 percent of fatal shootings stemmed from a traffic stop, slightly more than 14 percent from what officers deemed suspicious activity, and about 16 percent from domestic disturbances (see Table 1).[5] Furthermore, it might be advisable to consider the well-established age-crime curve, which suggests criminal behavior (and in turn, the risk of arrest) peaks in a person's 20s and declines thereafter.[6] However, the likelihood of being fatally shot by a police officer appears to increase from the early 20s to the late 30s, with many individuals in their 40s and 50s being fatally shot in police encounters, as well (see Figure 1). Relatedly, UCR data routinely show that females account for roughly 20 percent of all arrests, yet according to the *Washington Post*, they account for less than 5 percent of OIS fatalities. In other words, determining a proper denominator is difficult at best. While arrest data are arguably more suitable denominators than the general population, they are by no means perfect.[7]

Table 1. Fatal shootings by incident type, 2015 – 2017.*

Incident Type	N	%
Crime in progress	753	25.88
Domestic disturbance	466	16.01
Suspicious activity	411	14.12
Traffic stop	339	11.65
Other	320	11.00
Serving warrant	255	8.76
Suicidal person	167	5.74
Patrol	107	3.68
Unknown	92	3.16
Total	**2,910**	**100.00**

***Note:** Data obtained on 12/21/2017.

Using the Right Benchmark to Compare Jurisdictions

Because of the controversy surrounding OIS and a problematic lack of information on the topic, the researchers took a closer look at data recently collected by *VICE News* in search of a benchmark that might explain variations between jurisdictions in terms of the number of OIS. *VICE News* reached out to the 50 largest U.S. police departments and obtained data from 2010 to 2016 on all OIS—fatal and nonfatal—from 47 agencies.[8] These data were then merged with UCR data covering the same time period.

Figure 1: Age distribution of civilians fatally shot by police, 2015–2017. (N=2,876)

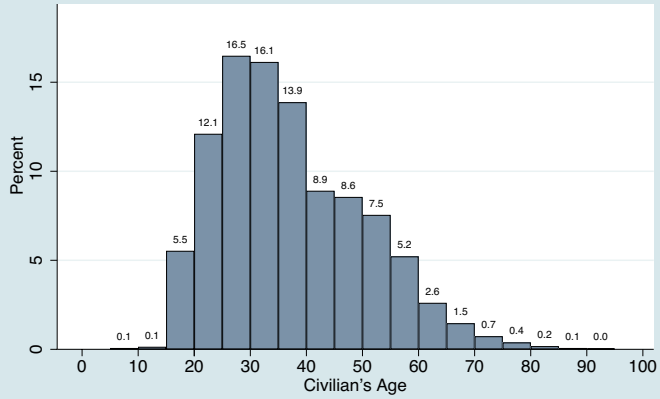
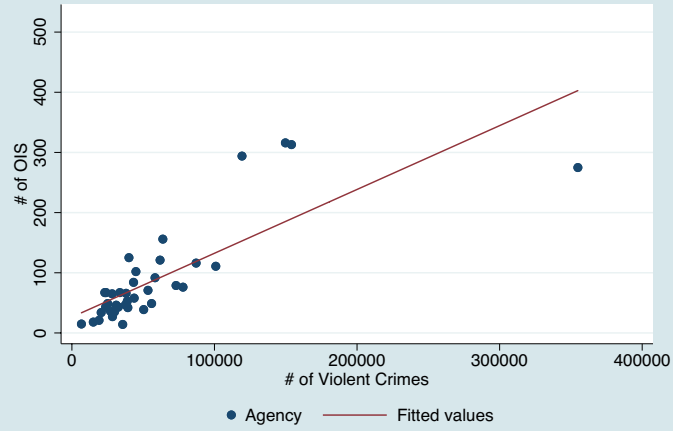
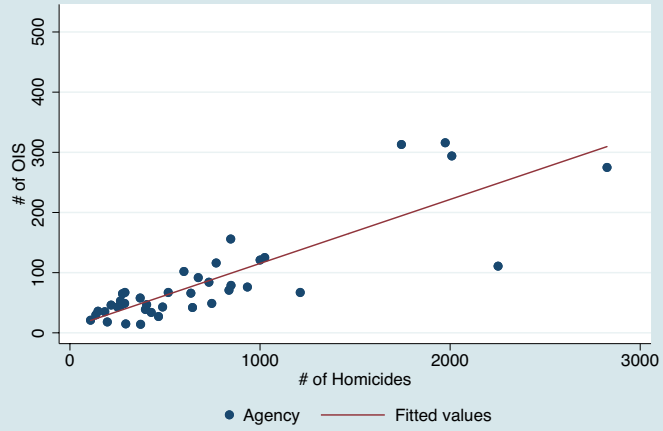


Figure 2: Number of OIS vs. Number of Violent Crimes, 2010–2016*



***Note:** Eight agencies were missing violent crime data for one or more years. As a result, this graph includes only 39 of the 47 agencies.

Figure 3: Number of OIS vs. Number of Homicides, 2010–2016*



***Note:** Seven agencies were missing homicide data for one or more years. As a result, this graph includes only 40 of the 47 agencies.

Once the data were merged, the number of OIS was plotted against the number of known violent crimes for each jurisdiction. As reflected in Figure 2, jurisdictions that experienced more violent crime have more OIS. To explore the relationship between crime and OIS in more detail, the researchers then plotted the number of OIS against the number of known homicides and found a stronger relationship (see Figure 3). While these are simple bivariate relationships at the jurisdiction level—which might be complicated by other important variables or mask neighborhood-level variation—these findings do square well with prior research that has been conducted with single agencies.[9]

Each OIS and every round fired must be evaluated for its legal and strategic justification. Once data are compiled on all OIS and an appropriate denominator is agreed upon, the context of OIS can be better understood. A measure of arrest data is a good way to begin the conversation, but must not end it. ❖

The opinions expressed in this article are those of the author(s) and do not necessarily represent the views of the IACP. The presence of this content in Police Chief *does not indicate endorsement by the IACP.*

Notes:

[1]See Justin Nix et al., "A Bird's Eye View of Civilians Killed by Police in 2015," *Criminology & Public Policy* 16, no. 1 (2017): 309–340.

[2]Amber Askey et al., "Insights on Officer Safety from Officer-Involved Shooting and Near Miss Incidents," *Police Chief* (May 2018): 42–45.

[3]Samuel Walker, "Searching for the Denominator: Problems with Police Traffic Stop Data and an Early Warning System Solution," *Justice Research and Policy* 3, no. 1 (2001), 63–95; Geoffrey P. Alpert, Michael R. Smith, and Roger G. Dunham, "Toward a Better Benchmark: Assessing the Utility of Not-at-Fault Traffic Crash Data in Racial Profiling Research," *Justice Research and Policy* 6, no. 1 (2004): 43–69.

[4]Charles R. Epp, Steven Maynard-Moody, and Donald P. Haider-Markel, *Pulled Over: How Police Stops Define Race and Citizenship*, Chicago Series in Law and Society (Chicago, IL: University of Chicago Press, 2014); Tammy Rinehart Kochel, David B. Wilson, and Stephen D. Mastrofski, "Effect of Suspect Face on Officer's Arrest Decisions, *Criminology* 49, 473–512.

[5]See Gillian M. Pinchevsky and Justin Nix, "Domestic Disturbances and Fatal Police Shootings: An Analysis of the Washington Post's Data," *Police Quarterly* 21, no. 8 (October 2017).

[6]David P. Farrington, "Age and Crime," *Crime and Justice* 7 (1986): 189–250.

[7]For more on arrests and fatal OIS, see Franklin E. Zimring, *When Police Kill* (Cambridge, MA: Harvard University Press, 2017), 44–48.

[8]See "Get the Data," *Vice News*, December 10, 2017, https://news.vice.com/en_us/article/a3jjpa/nonfatal-police-shootings-data.

[9]For example, David Klinger et al., "Race, Crime, and the Micro-Ecology of Deadly Force," *Criminology & Public Policy* 15, no. 1 (2016): 193–222.

FURTHER READING

To read more about the OIS Data Collection Initiative mentioned in this article, see "Insights on Officer Safety from Officer-Involved Shooting and Near Miss Incidents" in the May 2018 *Police Chief* (pages 42–45) or access it online at www.policechiefmagazine.org/insights-officer-safety-ois-near-miss.

Life After *Liverman*: Continuing to Police Employee Speech on Social Media

By Eric R. Atstupenas, Esq., General Counsel, Massachusetts Chiefs of Police Association

Life after *Liverman v. City of Petersburg* is not as bleak as it seems.[1] True, the purpose of *Liverman* was to provide a "shot across the bows" to public employers, warning that broad prior restraints in social media policies will not be tolerated. However, the "shock and awe" effects of the 2016 decision have been overreactions, in some instances, causing agencies to surrender entirely in the realm of policing their employees' online speech. But, complete surrender is not the answer ... there is life after *Liverman*.

The Knee-Jerk Reaction to *Liverman*

In *Liverman*, the U.S. Court of Appeals for the Fourth Circuit held that the City of Petersburg, Virginia, Police Department's social networking policy violated the First Amendment. Two provisions in the policy were the primary focus of the court's scrutiny: the Negative Comments Provision and that which "strongly discourages employees from posting information regarding off-duty activities."[2] Citing these two provisions, the court denied qualified immunity for the Petersburg chief of police on the grounds of the "patent overbreadth of the policy."[3] The knee-jerk reaction of many agencies across the United States was to scrap their social media policies entirely following this decision. Other agencies have read the decision as an outright prohibition against disciplining officers for online speech.

Clarifying *Liverman*

The *Liverman* decision is not all that groundbreaking. The decision does nothing with respect to the analysis that is used to determine what statements made by public employees are protected by the First Amendment. Indeed, public employees may not "be compelled to relinquish the First Amendment rights they would otherwise enjoy as citizens to comment on matters of public interest."[4] However, that is not the end of the analysis. A public employee's speech may be protected under the First Amendment only if (1) the employee was not speaking pursuant to his or her ordinary job duties; (2) the employee was speaking on a matter of public concern; and (3) the employee's interests outweigh the interests of the employer.[5]

Further, the analysis used to determine the constitutionality of social media policies remains unchanged. The analysis used by the *Liverman* court closely tracks the same test previously announced by the U.S. Supreme Court, requiring that a more stringent standard be applied to instances involving a prior restraint which "chills potential speech before it happens."[6] The application of that standard to the policy in *Liverman* could produce only one conclusion: the policy as a whole was unconstitutionally overbroad. Despite this determination, the focus of the scathing opinion was primarily on the Negative Comments Provision and the provision that strongly discouraged officers from posting regarding off-duty activities. The *Liverman* court was substantially more accepting of the Public Concern Provision in the policy, which was "ostensibly more aligned with the case-by-case analysis of *Connick* and *Pickering*."[7] However, in light of the aforementioned unconstitutional provisions, the court could not uphold the validity of the social media policy on the existence of the Public Concern Provision alone.

Finally, the doctrine of qualified immunity remains the same. Admitting that officials "are not liable for bad guesses in gray areas," the court retorted that "this case does not involve gray areas: the right against such a sweeping prior restraint on speech was clearly established and then some."[8] Undeniably, portions of the social media policy at issue clearly impeded employees from engaging in constitutionally protected speech, and portions of the policy could be read as prohibiting employees from posting anything on social media whatsoever. In such instances, the argument for qualified immunity would be tenuous, at best.

In the Wake of *Liverman*

Law enforcement agencies should continue to monitor the online speech of their employees utilizing the same analysis discussed above. U.S. agencies should also work closely with their respective legal advisors to either implement a constitutionally compliant social media policy or to make the necessary adaptations to an existing policy. While agencies may use the "conduct unbecoming" charge to resolve incidents involving employee speech online, social media policies have the advantage of providing both the employer and employee with at least a baseline for the applicable standards and an understanding of what conduct is and is not acceptable. Utilizing both the "conduct unbecoming" charge and the social media policy may prove to be the most effective approach.

A social media policy should be crafted to prohibit only that conduct that is not protected by the First Amendment. For example, social media policies may prohibit employees from displaying department logos, uniforms, or photographs that cause the individual to be identified as a police officer of the department or from accessing social media while on duty. The policy should also contain guidelines as to when disciplinary action may be taken for employee content on social media. Policies may advise that personnel are free to express themselves as private citizens speaking on matters of public concern, but that employees should be careful not to conduct themselves in a manner that impairs the maintenance of discipline by supervisors, impairs working relationships of the department, impedes the performance of duties, impairs discipline and harmony among coworkers, interferes with department operations, undermines the department's mission, conflicts with personnel responsibilities, amounts to an abuse of authority, or undermines public accountability. The policy should make it clear that the decision and degree to which discipline is imposed will be determined on a case-by-case basis.

Conclusion

Liverman serves as a catalyst for agencies to dust off their social media policies and make such necessary revisions to comply with the First Amendment, as opposed to depositing them in the "circular file" altogether. *Liverman* should not be read to discourage agencies from continuing to police employee speech on social media, solely to ensure that the appropriate standards are applied. ❖

Notes:

[1]*Liverman et al. v. City of Petersburg et al.*, 844 F.3d 400 (4th Cir. 2016).

[2]"Negative comments on the internal operations of the Bureau, or specific conduct of supervisors or peers that impacts the public's perception of the department is not protected by the First Amendment free speech clause, in accordance with established case law." *Liverman*, 844 F.3d at 404.

[3]*Liverman*, 844 F.3d at 414.

[4]*Pickering v. Bd. of Educ.*, 391 U.S. 563, 568 (1968).

[5]*Pickering*, 391 U.S. 563; *Connick v. Myers*, 461 U.S. 138, 149 (1983); *Lane v. Franks*, 134 S. Ct. 2369, 2378 (2014); *Garcetti v. Ceballos*, 547 U.S. 410, 418 (2006).

[6]*Liverman*, 844 F.3d at 407; *United States v. Nat'l Treasury Employees Union* (NTEU), 513 U.S. 454, 468 (1995).

[7]*Liverman*, 844 F.3d at 409. "Officers may comment on issues of general or public concern (as opposed to personal grievances) so long as the comments do not disrupt the workforce, interfere with important working relationships or efficient work flow, or undermine public confidence in the officer. The instances must be judged on a case-by-case basis." *Liverman*, 844 F.3d at 404.

[8]*Liverman*, 844 F.3d at 411, in part citing *Maciariello v. Summer*, 973 F.2d 295, 298 (4th Cir. 1992).

POLICY RESOURCE

IACP's Law Enforcement Policy Center serves as a resource for law enforcement executives and policy makers seeking to update or establish new polices at their agencies. Available to IACP members, the model policies cover a wide range of topics, including investigations, officer safety, personnel, use of force, and other areas of interest.

The Policy Center can be accessed at www.theIACP.org/model-policy.

PLANNING, DESIGNING, AND CONSTRUCTING POLICE FACILITIES COURSE

Looking to design a new facility or update your current building?

THIS COURSE IS FOR YOU.

Discuss planning considerations for facility construction.

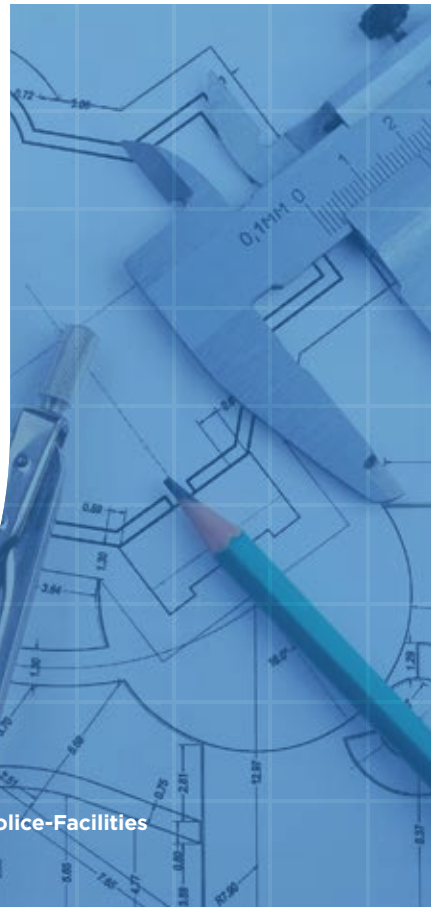
Plan and budget for a new or redesigned police facility.

Plan special design features such as security, jails, and communications.

Understand the implications of sustainable (green) design principles.

Develop effective client-architect relationships.

Identify life span and maintenance considerations for a facility.



125 Years 1893 - 2018 IACP International Association of Chiefs of Police

Training@theIACP.org

theIACP.org/Planning-Designing-and-Constructing-Police-Facilities

LexisNexis® | Coplogic™ Solutions

CASE STUDY

Getting Into High GEARS: Police in LaGrange, Georgia Use Crash-Reporting Technology to Manage Resources, Maintain Public Safety

Advances in automobile crash reporting technology are helping law enforcement agencies across the country to better manage resources and keep their jurisdictions safe. One of the places where this is happening is LaGrange, Georgia, where Chief Louis Dekmar and the LaGrange Police Department have been leaders in improving traffic safety in their community.

By applicable state laws, crash data is collected by police departments statewide and sent to the state crash repository maintained by the Georgia Department of Transportation. Prior to 2009, that data was collected using paper forms, and months or years could pass before it was manually entered into an antiquated computer system.

"Police collect a lot of information," said Chief Dekmar, "but the challenge is getting that information out in a way that allows you to affect public safety and traffic." Due to the lag that existed between data collection and its eventual availability, police, local elected officials, and other public safety stakeholders were hamstrung in their ability to make data-driven decisions in a timely way.

When Georgia adopted a statewide system called Georgia Electronic Accident Reporting System (GEARS) to collect, store and analyze crash data, LaGrange, situated near the state's western border, was one of the first law enforcement agencies in the state to make use of the new technology. "It was about being able to use [data] in a way that better serves your community," said Chief Dekmar.

Why data matters

Vehicle crash data serves a number of functions in law enforcement and public safety. Highway research and safety groups make use of it when they ask for traffic studies, transportation agencies and elected officials rely on it when planning new routes or putting traffic-calming devices in place, and for law enforcement officials and organizations like Chief Dekmar and the LaGrange Police Department, it is a vital need in order to make informed decisions about how to best deploy officers and resources.

Using data to boost efficiency

Historically, according to Chief Dekmar, crash data had to be processed manually and could take a significant amount of time to make its

way into an accessible format. “Technology was paper and a pen. That was technology,” Chief Dekmar said of his beginnings in law enforcement. “I came in 40 years ago: 27 years as police chief and 40 years in policing, so yes, of course it was all paper.” Officers would have to return to the station and transfer information from paper reports using desktop PCs, transitioning to laptops only in the late 1990s to early 2000s.

This was a common situation among Georgia law enforcement agencies until the state implemented GEARS in 2009. Developed by a company that would eventually become a part of LexisNexis Risk Solutions, GEARS was one of the first statewide electronic crash reporting systems in the nation. And, due in part to a briefing on the new technology delivered to board members of the Georgia Association of Chiefs of Police, Chief Dekmar was eager to take advantage of the solution and put it to use in LaGrange.

One of the major impacts of GEARS has been increased efficiency in deploying traffic enforcement personnel to high-priority locations. Chief Dekmar said, “We want fifty percent of our citations written in areas of the city where we have the most accidents or complaints. And GEARS certainly provides the guidance in assigning those areas.”

Saving time and resources

Another advantage is a reduction in staff time spent analyzing data. “Given the size of our agency, we can’t afford to have somebody spend a day or two pouring through [crash data],” said Chief Dekmar, adding that LaGrange had 2,444 accidents in the previous year. Analysis at this volume level would significantly cut into time better spent on more critical tasks.

Achieving results: public service and public safety

Chief Dekmar said the response to electronic reporting has been positive, cutting down on the need to make an in-person visit to the police department.

The additional speed and efficiencies provided by GEARS have had concrete impact on Chief Dekmar’s department and on public safety in the city. The LaGrange Police Department has improved its ability to allocate officers and resources effectively in order to be responsive to citizens. Chief Dekmar said, “The expectations of the police are always expanding, and there are fewer social controls, whether they be in family, or community, or neighborhood, or education. The substitute for that when things go bad is always more police presence or more police involvement. You leverage everything you can in order to get those resources, and of course taking advantage of technology is one of those ways.”

“Our citizens receive the benefit of better enforcement and safer roads,“ said Chief Dekmar. “GEARS is one piece of the puzzle that helps us improve traffic safety in our community.”

LexisNexis and the Knowledge Burst logo are registered trademarks of RELX Inc. Coplogic is a trademark of LexisNexis Claims Solutions, Inc. Other products and services may be trademarks or registered trademarks of their respective companies. Copyright © 2018 LexisNexis.

PROTECTING THE POWERLESS: Combating Cyber Child Sexual Exploitation

By John F. Clark, President and CEO, The National Center for Missing & Exploited Children

"Every day of my life I live in constant fear that someone will see my pictures and recognize me and that I will be humiliated all over again. It hurts me to know someone is looking at them—at me—when I was just a little girl being abused for the camera. I did not choose to be there, but now I am there forever in pictures that people are using to do sick things. I want it all erased. I want it all stopped. But I am powerless to stop it just like I was powerless to stop my uncle."[1]

—Victim whose sexual abuse began at age four

This is just one voice, but tens of thousands of other survivors of child sexual abuse, if not more, share the same debilitating fear that photos and videos memorializing their sexual abuse as a child will forever remain on the Internet for anyone to see. Every time an image is viewed, traded, or downloaded, that person is re-victimized, often well into adulthood.

Now, there's hope for these survivors. Leaders in the technology industry like Google, Facebook, Palantir, Microsoft, and Intel are helping to reduce the proliferation of these images online and developing new ways to prevent future victimization. What was once thought to be impossible is now possible.

With help from the National Center for Missing & Exploited Children (NCMEC), online technology companies have developed effective tools and procedures to track down these exploitative images wherever they may be on the Internet and take them down. While it is impossible to take away a child's experience of enduring sexual abuse, NCMEC and its technology partners

are working tirelessly to prevent the revictimization of those children.

The NCMEC team sees these abuse images every day and recognizes their long-term psychological impact on survivors. For more than 34 years, this 24/7 nonprofit has been at the forefront of child protection, and, in recent years, NCMEC has witnessed an explosion in child sexual exploitation on the Internet.

For 20 years, NCMEC has operated the CyberTipline. During that time, the nonprofit has received more than 27 million reports of suspected child sexual exploitation, more than half of which are from just the last two years.[2] Reports concerning all kinds of sexual abuse of children continue to come in, but the vast majority of them are for child sexual abuse images and videos.

The Internet has become an integral and invaluable part of society today, but it also has a dark underbelly. It's become a secure environment for people with like-minded, dark interests to produce and share images with one another. Moreover, it has shined a spotlight on the seemingly insatiable demand for sexually abusive images of children.

NCMEC's CyberTipline serves as a centralized mechanism for reporting child sexual exploitation. The reports are reviewed by NCMEC analysts, who try to determine where these crimes are happening, then make them available to the appropriate law enforcement agency for potential investigation. The organization also sends reports to more than 100 police forces around the world, including Europol and Interpol.

Upon request from law enforcement, NCMEC also reviews collections of seized child pornography to determine which images depict child victims already identified by law enforcement. In addition, the nonprofit helps law enforcement locate previously unidentified victims so they can be rescued from abusive situations.

NCMEC's dedicated staff has analyzed hundreds of millions of these images and videos, many of them homemade, looking for clues that might help law enforcement determine, literally, where in the world is this child? Where are these images being produced?

The number on a Brownie uniform slung over a chair, a TV left on in the background, or a receipt lying on a desk are just some of the clues that have helped lead law enforcement to these sexually abused children. And law enforcement is doing a commendable job investigating these cases. As of this date, police have asked NCMEC to analyze more than 235 million child sex abuse images and videos.

"[W]e can never forget that the victims depicted in child pornography are real children and the images are evidence of their sexual abuse," explains Michelle DeLaune, chief operating officer for NCMEC.[3]

Once a child has been rescued from an abusive situation, law enforcement learns the story behind the image. They learn that these children live in our communities. They may play on our child's baseball team, dance in our child's ballet class, or sit next to our child on the school bus.[4]

The CyberTipline has given NCMEC a unique lens into who these children are and how they're being sexually exploited. This information and experience shapes the organization's safety tips and prevention programs.

Who Are the Children in Sexual Abuse Images?

Since NCMEC began receiving these sexual abuse image reports 20 years ago, there's always been a demand for sexual abuse images of very young children. Of the children who've been identified, more than 70 percent are girls. Nearly 40 percent are prepubescent, typically under 10 years old, and more than 5 percent are infants or toddlers.[5]

Most of the children in these photos and videos have been abused by someone they know, whether a family friend, a parent, or another relative. They're often sexually abused in their own homes or the homes of someone they know. These are not "baby in a bathtub" photos; they are violent and graphic images of unimaginable abuse.

Impact on Victims

Victims of child pornography are often traumatized from the sexual abuse inflicted on them. That harm is compounded when the abuse is memorialized with photos and videos and distributed on the Internet for the viewing pleasure of others. These children also suffer knowing that their images may be used to entice or manipulate other children into sexually abusive acts.

One child victim, now an adult, told the court,

When I was told how many people have viewed these images and videos I thought my pulse would stop. Thinking about all those sick perverts viewing my body being ravished and hurt like that makes me feel like I was raped by each and every one of them.[6]

To better understand the long-term psychological impact to these victims, NCMEC partnered with the Canadian Centre for Child Protection on its survey of adult survivors whose child sexual abuse was recorded and potentially distributed online. The 150 survivors who took the ongoing survey as of September 2017 are all struggling mightily.[7]

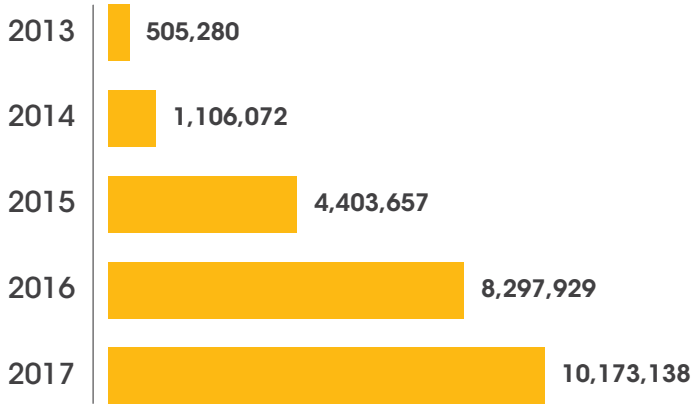
These survivors said their sexual abuse as children has significantly reduced their ability to cope with day-to-day stresses, maintain healthy relationships, and reach their full potential in educational and occupational pursuits. They worry constantly about being recognized by someone who has seen their images.

Most of these survivors were sexually abused when they were very young children and didn't report the abuse because they were afraid. For those who did tell someone, they were not always believed, and the abuse continued. The survey also revealed that the Internet has provided an opportunity for offenders to connect and work together in an organized way to form communities where they conspire to commit more sex acts on children and share or trade these images.

Sextortion

For the past five years, NCMEC has been tracking a relatively newly identified form of child sexual exploitation known as "sextortion." In these cases, the offenders use nonphysical forms of coercion, including blackmail, to acquire sexual images or videos of the child.

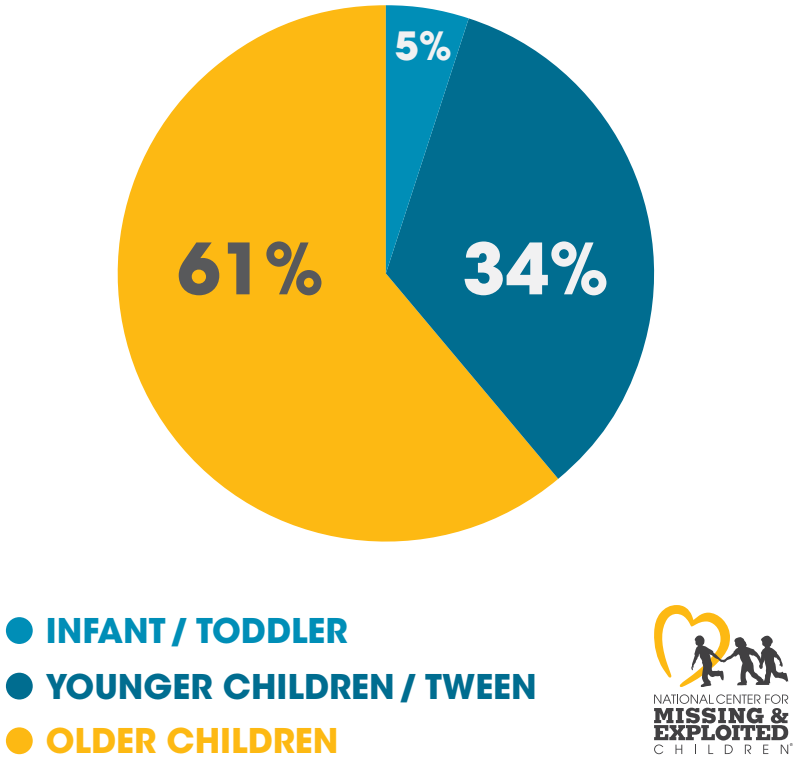
Figure 1: CyberTipline Child Abuse Reports



NATIONAL CENTER FOR MISSING & EXPLOITED CHILDREN

In 2017, the CyberTipline received a record 10.1 million reports

Figure 2: Child Pornography: Ages of Victims



A 2016 report issued by NCMEC analyzed 1,428 sextortion reports made to the CyberTipline. Most victims were girls, but boys were also victims of sextortion. The children were as young as 8, with an average age of 15. Offenders target these children on multiple platforms, including messaging apps, social networking sites, and video chats.[8]

With so much technology available to children today, these offenders have an easy—and seemingly anonymous—way to connect with children and develop their trust, even in the perceived safety of the children's own homes. That ease of access, coupled with the normal curiosity of children, presents fertile ground for these types of crimes. Offenders use different tactics to gain a child's trust. Some will groom the children by pretending to develop a friendship or romantic relationship. In some cases, offenders will offer the child gifts or pretend to work for a modeling agency.

Once the offenders gain a child's trust, they begin coercing the child into sending them sexually explicit images. This often leads to threats that they'll post previously acquired images online in a place where family and friends can see them if the child doesn't comply with further demands.

Offenders have also used other ways to get what they want, including threatening to hurt the child or the child's family members or secretly recording sexually explicit videos of the child during video chats to use as blackmail. Some have even threatened to create sexual images of the child by Photoshopping the child's face with another person's body or to commit suicide if the child doesn't send them images.

Feeling alone, and too afraid to seek help, these young victims often exhibit hopelessness, anxiety, and depression. One third of the children experiencing sextortion who experienced these feelings of hopelessness, depression, fear, and anxiety have engaged in self-harm, threatened suicide, or attempted suicide as a result of the victimization.[9] Tragically, some have killed themselves.

Ashley Reynolds was 14 when a stranger wrote in the subject line of a message that he had naked pictures of her. He kept messaging her, demanding sexually explicit photos and threatening to ruin her reputation if she didn't do what he said.

She was frightened and sent a few sexually explicit photos, then a few more. And more. And more. Very quickly, she had become ensnared in a sextortion scheme, and her torment lasted for months. Ashley was being held hostage in her own home.

Fortunately, her mother discovered what was happening and reported it to NCMEC. The FBI not only located and successfully prosecuted the offender, but uncovered computer records showing he had terrorized nearly 350 other girls in the United States, Canada, and the United Kingdom.[10]

In 2016, at NCMEC's annual "Hope Awards," Ashley was honored for her courage in taking on a predator and going public about her ordeal in hopes of helping other children and educating parents. "I was virtually kidnapped," said Ashley. "I was abducted by a stranger. My parents saw me every single day, but they had no idea."[11]

What NCMEC Is Doing to Help These Child Victims

NCMEC, seeing these children being continually revictimized, began challenging the prevailing belief that once something has been posted on the Internet, it's impossible to take it down. With all the advances in technology, NCMEC wondered if there was some way to reduce the tsunami of sexually explicit images and help these tormented victims and their families.

NCMEC met with the technology industry to see if there might be a way to do this. Could digital fingerprints or hash values, be the answer? After all, every image has a unique digital fingerprint. Perhaps, if NCMEC compiled a list of hash values, they could share them with Internet service providers. The technology companies would then be able to delete them if known child abuse material is hosted on their network.

Hashing technologies had some serious limitations, though. If an image of a child was altered just the slightest bit—removing red eye, resizing the photo, even adding a pixel—the hash values wouldn't match, even if it was the same child. It was back to the drawing board.

However, what eventually emerged in 2008 was one of the most powerful, significant tools created for reducing child sexual abuse images online: PhotoDNA.

Microsoft, in collaboration with Dartmouth College, developed a precise image-matching technology, creating a PhotoDNA "fingerprint" that is resistant to alterations. This voluntary initiative with online companies has continued to grow annually, and more photos are being surgically plucked from a sea of images. More and more companies are signing on, taking a zero-tolerance approach to the presence of these images on their platforms. As a result, reports to the CyberTipline in 2015 began to skyrocket.

"The widespread adoption of these technology tools speaks to the extremely precise nature in which technology companies can identify and remove content," said John Shehan, who oversees NCMEC's Exploited Children Division. "This surgical-like precision takes into account the need to quickly and proactively find the heinous illegal material, while balancing the privacy concerns of legitimate Internet users."[12]

NCMEC also began proactively notifying these companies when it became aware of sexually abusive images on their websites, sending alerts to the providers hosting

the content. Last year alone, NCMEC sent 56,565 notifications, and these companies are now taking down these vile images in a matter of hours, bringing immense psychological relief to victims.

NCMEC recently partnered with the Canadian Centre for Child Protection, which has developed an exciting new tool. It can detect where these child sex abuse images are publicly available on the Internet—but at lightning speed and on a much larger scale than current methods. The automated crawler, called Project Arachnid, detects images and videos of both identified and unidentified victims. It's a game changer.

In just a six-week period, Project Arachnid processed over 230 million webpages and detected more than 5.1 million unique webpages hosting these images of child sexual abuse.[13]

"There is much work to do," said Shehan. "But we're confident that the collective will exists to stop the revictimization of these survivors."[14] ❖

For more information about NCMEC resources, go to www.missingkids.org and www.missingkids.org/training. To report child sexual exploitation, go to www.cybertipline.org.

Before **John F. Clark** became CEO and president of NCMEC, he was director of the U.S. Marshals Service for five years. His career with the USMS spanned 28 years.

Sextortion survivor and crusader, Ashley Reynolds, takes the podium at 2016 NCMEC Hope Awards.

Notes:

[1]"Document: Victim Impact Statement of Girl in Misty Series," *The Virginian-Pilot*, October 25, 2009, https://pilotonline.com/news/article_d36e144a-7bc6-5c77-a780-502003a404da.html.

[2]National Center for Missing and Exploited Children (NCMEC), "CyberTipline," http://www.missingkids.com/gethelpnow/cybertipline.

[3]*Federal Child Pornography Offenses, Before the U.S. Sentencing Commission* (2012) (testimony of Michelle Collins, vice president, Exploited Children Division, and assistant to president of NCMEC).

[4]Michelle DeLaune (senior vice president and COO, NCMEC), interview, March 2018.

[5]NCMEC, internal CyberTipline data, 2018.

[6]Middle District of Alabama, U.S. Attorney's Office, "Child Molester Nets 40-Year Sentence Under New Federal Anti-Grooming Law," press release, July 15, 2009, https://archives.fbi.gov/archives/mobile/press-releases/2009/mo071509a.htm.

[7]Canadian Centre for Child Protection, "First of Its Kind Data on the Role of the Internet and Its Impact on Child Sexual Abuse," news release, September 26, 2017, https://www.cybertip.ca/app/en/media_release_201709_survivors_survey_results.

[8]NCMEC, "Sextortion," http://www.missingkids.com/theissues/onlineexploitation/sextortion.

[9]NCMEC, "Sextortion."

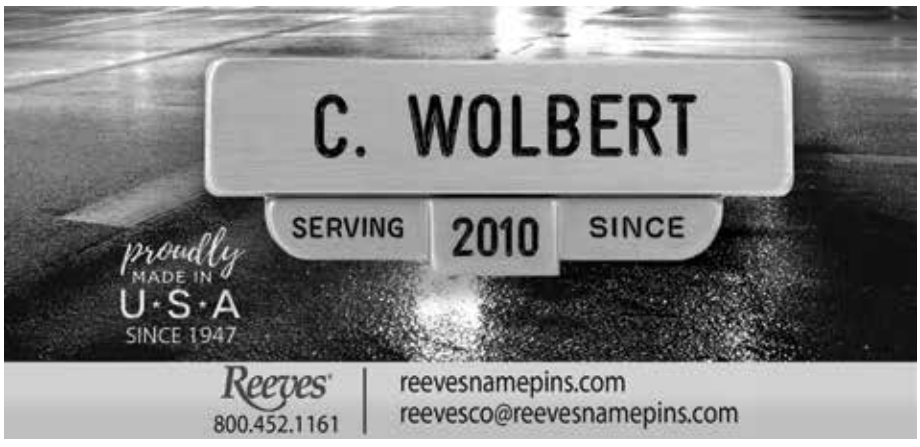
[10]Liz Brody, "Meet Ashley Reynolds, the Woman Fighting 'Sextortion,'" *Glamour*, July 7, 2015, https://www.glamour.com/story/ashley-reynolds-the-woman-fighting-sextortion.

[11]Barbara Worth, "Sextortion, Technology, Philanthropy Heroes Honored at NCMEC Hope Awards," *NCMEC* (blog), May 13, 2016, http://blog.missingkids.com/post/144281997220/sextortion-technology-philanthropy-heroes.

[12]John Shehan, "Eliminating Child Sexual Abuse Material: The Role and Impact of Hash Values," *Thorn Blog* (blog), April 18, 2016, https://www.wearethorn.org/blog/eliminating-child-sexual-abuse-material-hash-values.

[13]Cybertip.ca, "Project Arachnid," https://www.cybertip.ca/app/en/projects-arachnid.

[14]John Shehan (vice president. Exploited Children Division, NCMEC), interview, March 2018.



Following the Money: Investigating Cryptocurrency

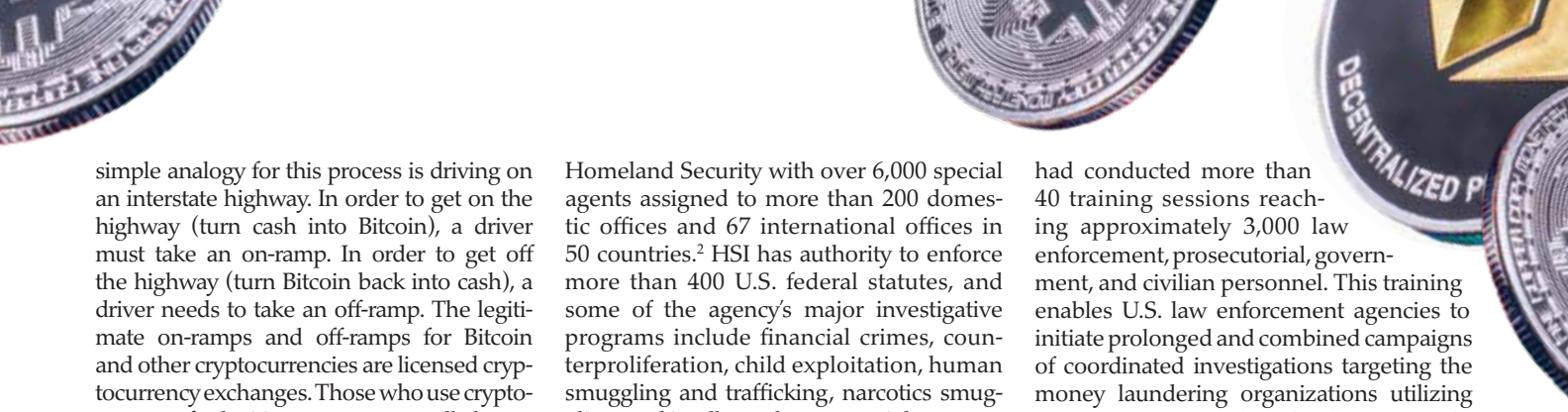
By John Hedrick and Jeremy Bluto, Program Managers, Homeland Security Investigations, Illicit Finance and Proceeds of Crime Unit

When Bitcoin, the first decentralized cryptocurrency, was issued in 2009, an entirely new world was created in relation to money laundering and financial investigations. Bitcoin, at the simplest level, is a peer-to-peer (P2P) electronic payment system that does not require a third party to process a transaction. Bitcoin was initially created with the intention of providing banking services to the unbanked, while creating a faster and less expensive way to send money anywhere in the world. Today, Bitcoin is accepted as a method of payment by hundreds of traditional merchants and is also widely used by many criminal organizations. There are currently more than 1,550 different cryptocurrencies in existence. Bitcoin is, by far, the largest and most widely accepted cryptocurrency with a market capitalization, of more than $163 billion, as of May 2018.[1]

Following its introduction, Bitcoin quickly became the currency of choice on the dark net as buyers and sellers enjoyed the pseudo-anonymity it provided. Silk Road, the first major dark net marketplace, was taken down by a joint law enforcement operation in which Homeland Security Investigations (HSI) was a lead agency. Since then, many more dark net marketplaces have emerged and subsequently been taken down by law enforcement. The dark net operates within the larger deep web, and services such as The Onion Router (TOR) are designed to provide and enhance the anonymity of its users. HSI works to combat the constantly emerging dark net marketplaces and the cryptocurrencies that drive them by utilizing both new and traditional investigative techniques and following the money. HSI does not treat the use of cryptocurrency for illicit purposes as a cybercrime, but rather an online-enabled financial crime.

Cryptocurrencies live on blockchains. A blockchain is a distributed public ledger where every transaction conducted using the specific cryptocurrency is recorded. This public ledger or blockchain at least in the case of Bitcoin, is open and available to be viewed by the public. Anyone with an Internet connection can query the blockchain for the details about any and every transaction. The fact that the Bitcoin blockchain is public means that law enforcement has the same access to transactional data as the rest of the world, and there is no subpoena, warrant, or other legal process needed. That transparency makes following the money easier than ever before. For instance, if law enforcement knows the Bitcoin address of one bad actor, the addresses of every other person the bad actor has conducted a transaction with is just a few mouse clicks away. Unfortunately, the challenge is that a Bitcoin address does not contain any information about the person or persons who control the address. This is what gives Bitcoin its pseudo-anonymity characteristic.

Despite the pseudo-anonymity enjoyed by the users of Bitcoin and other cryptocurrencies, as well as the ease in which the currencies can be transferred, at some point criminals need to convert their cash into Bitcoin or their Bitcoin into cash. The



simple analogy for this process is driving on an interstate highway. In order to get on the highway (turn cash into Bitcoin), a driver must take an on-ramp. In order to get off the highway (turn Bitcoin back into cash), a driver needs to take an off-ramp. The legitimate on-ramps and off-ramps for Bitcoin and other cryptocurrencies are licensed cryptocurrency exchanges. Those who use cryptocurrency for legitimate purposes will choose a legitimate cryptocurrency exchange that is registered with the U.S. Department of the Treasury's Financial Crimes Network (FinCEN)—and usually with their state—and is compliant with anti-money laundering (AML) and Know Your Customer (KYC) regulations. Legitimate users are more than willing to provide personal identifying information and traditional financial institution account numbers in exchange for security, the lowest fees, and the ease of processing transactions. Those who use cryptocurrency for illegal purposes, however, stay away from licensed exchanges in an effort to conceal their own identities. Instead, these criminals look to illicit exchanges to on-ramp and off-ramp their money. These illicit exchanges often take the form of a direct P2P exchanger.

P2P exchangers post advertisements stating the price they are willing to either buy or sell cryptocurrency for on websites such as localbitcoins.com or even Craigslist. These P2P exchangers are required by U.S. federal law to register with FinCEN, as well as the states they operate in, if required by state law, and maintain compliance with all federal banking regulations. Although some P2P exchangers do register and follow compliance laws, most do not. Rather, these illicit P2P exchangers position themselves as the money launderers of the cryptocurrency world. One type of P2P exchanger illegally generates revenue by charging a premium for allowing their customers to remain anonymous. They will sell cryptocurrency above market value and buy below market value to or from those customers who want to remain anonymous. A second type of illegal P2P practice involves a person or entity that operates as a vendor on dark net marketplaces, operating as a P2P exchanger as a means to convert the cryptocurrency received as payment to the cash needed. These P2P exchangers will often sell their cryptocurrency below market value when they are rich in cryptocurrency, but poor in traditional currency.

HSI Cryptocurrency Investigations and Training

HSI stands at the forefront of combating transnational crime and actiors that seek to exploit U.S. travel, trade, and financial systems for illicit purposes. HSI is the lead investigative arm of the U.S. Department of Homeland Security with over 6,000 special agents assigned to more than 200 domestic offices and 67 international offices in 50 countries.[2] HSI has authority to enforce more than 400 U.S. federal statutes, and some of the agency's major investigative programs include financial crimes, counterproliferation, child exploitation, human smuggling and trafficking, narcotics smuggling, and intellectual property rights.

By following the money, HSI identifies where these criminals are most vulnerable. This is where the cyber and traditional investigative worlds merge. HSI has established itself as a leader in the development of online undercover strategies and other innovative investigative techniques. Utilizing traditional investigative methods such as surveillance, undercover operations, confidential informants, and analysis of financial records, along with blockchain analysis, HSI can identify and exploit chokepoints that reveal the identities of those using cryptocurrency for illegal purposes. Arresting and taking down illegal P2P exchangers helps to open the door and pull back the veil of pseudo-anonymity provided by cryptocurrencies. Through interviews and suspect cooperation, along with forensic analysis of computers, mobile phones, and other seized electronics, HSI can identify other criminals using cryptocurrency to fund and further their illicit activities.

Historically, HSI special agents have worked cooperatively with state, local, and international partners to investigate criminal networks operating around the globe by using long-established investigative techniques that have gradually evolved to keep pace with changing methodologies of transnational criminal organizations (TCOs). However, due to the rapidly increasing transformative nature of technology, it is more essential than ever that law enforcement agencies enhance their adaptability and fluidity when combating transnational crime. Nowhere is this more apparent than in the rapidly expanding world of cybercrime and online-enabled financial crime within the dark net. Like many agencies, HSI has been engaged in a multiyear effort to increase its "cyber-enabled" workforce by training special agents, intelligence analysts, and computer forensic analysts to conduct online investigations.

The HSI Illicit Finance and Proceeds of Crime Unit and the HSI Cyber Crimes Unit conduct cryptocurrency and dark web training for HSI agents and federal, state, local, tribal, and international partners. Special agents from HSI headquarters and field office subject matter experts conduct this specialized training. This training, called Cryptocurrencies and the Dark Web, has been well received and, as of May 2018, HSI had conducted more than 40 training sessions reaching approximately 3,000 law enforcement, prosecutorial, government, and civilian personnel. This training enables U.S. law enforcement agencies to initiate prolonged and combined campaigns of coordinated investigations targeting the money laundering organizations utilizing crypto-currencies to launder illicit proceeds. HSI will continue this training and intends to follow up this course with intermediate- and advanced-level training.

The Future of Cryptocurrency

Many new cryptocurrencies have been and will continue to be developed. In the future, cryptocurrencies will likely have features that make the tracing of them more complicated. These anonymity-enhanced cryptocurrencies (AECs) are being developed specifically for use on the dark net as an effort to prevent the exploitation of public blockchains. Although it is more difficult to trace the movement of illicit proceeds using these newer AECs, it is not impossible.

Technology will inevitably continue to evolve, and law enforcement agencies everywhere must continue to adapt and evolve as well. HSI will continue to partner with all law enforcement agencies, along with cutting-edge private technology partners, to stay ahead of the curve and keep technologically savvy criminals on their heels. These vital partnerships are the foundation that allows law enforcement to continue its effort in combating TCOs on all fronts, including the emerging threat of online-enabled financial crimes. ❖

For more information about HSI's training on cryptocurrencies, the dark web, and related topics, contact IFPCU Unit Chief Michael Buckley at michael.e.buckley@ice.dhs.gov or IFPCU Section Chief Lucy Escamilla at lucy.e.escamilla@ice.dhs.gov.

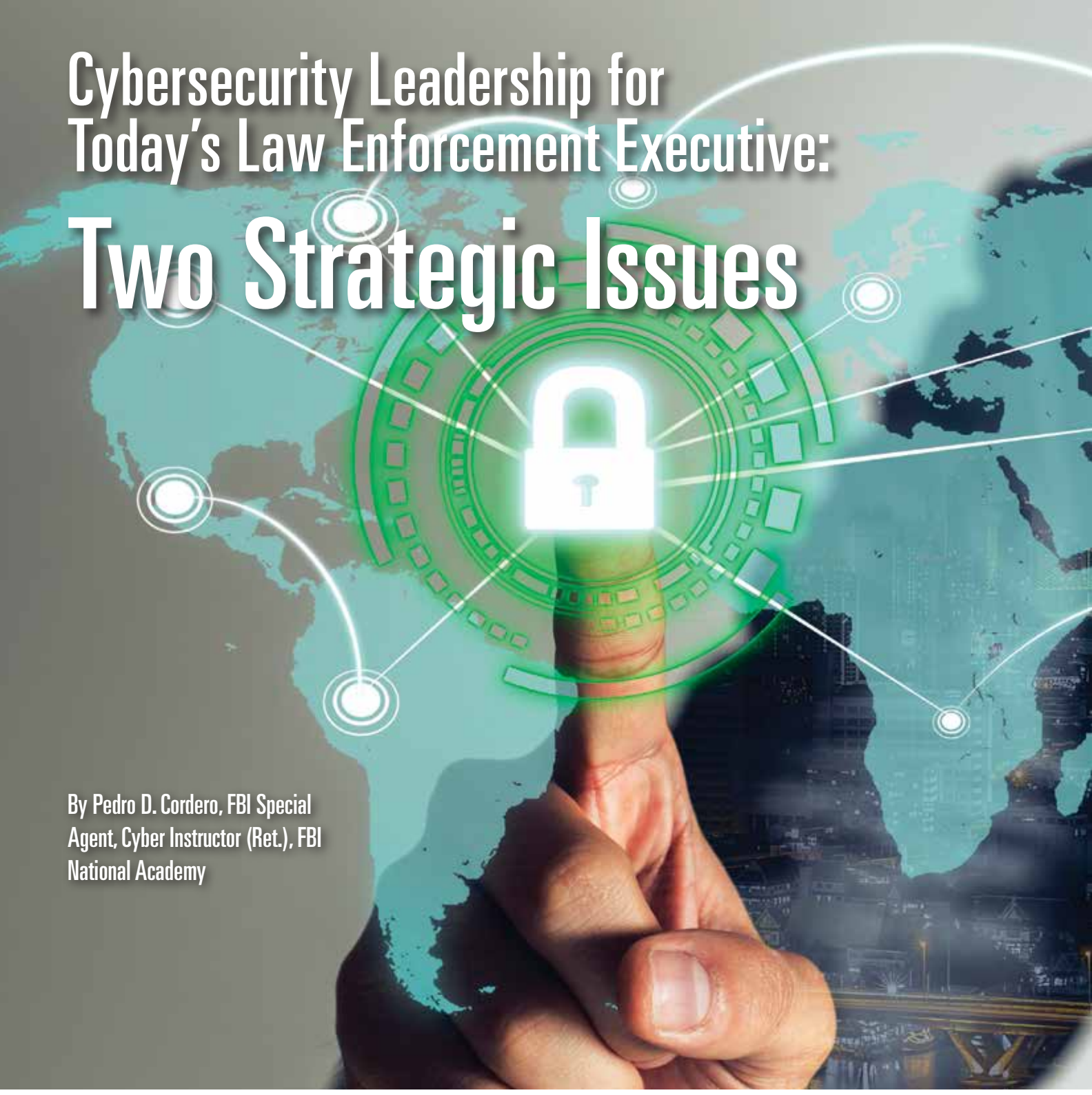
Notes:

[1]"Cryptocurrency Market Capitalizations," CoinMarketCap, https://coinmarketcap.com/all/views/all.

[2]U.S. Immigration and Customs Enforcement, "Frequently Asked Questions: What Is HSI?" https://www.ice.gov/careers/faqs.

Cybersecurity Leadership for Today's Law Enforcement Executive:

Two Strategic Issues



By Pedro D. Cordero, FBI Special Agent, Cyber Instructor (Ret.), FBI National Academy

Today's law enforcement leaders are regularly exposed to the multilevel impact of strategic cyberthreats. Daily news media coverage reports cyberattack incidents impacting both private and public sector organizations. Victims of these cyberattacks include such organizations as state, local, tribal, and territorial law enforcement agencies and all levels of government.

Two distinct strategic issues impact all law enforcement executives and their respective organizations. The first strategic issue is the acceptance of the overall responsibility for the cybersecurity posture of the law enforcement agency by chiefs and senior leadership teams. This issue requires chiefs and their senior leadership teams to be cyber-savvy leaders.

The second strategic issue is the need to create the organic capability to successfully investigate and prosecute cybercrimes and intrusions at the state, local, tribal, and territorial levels. This requires cyber-savvy law enforcement executives to strategically plan an operational organic cyber investigative capability with tactical cyber capabilities for their organization.

The Cyber-Savvy Law Enforcement Executive

How many of today's law enforcement executives are properly prepared for a strategic cyberthreat? Prepared or not, the threat is realistic, so law enforcement executives who are not properly

prepared to address the cybersecurity threat should consider transforming themselves to be cyber-savvy leaders for their agencies.

Are law enforcement executives naturally prepared to address threats such as counterterrorism, active shooter situations, weapons of mass destruction, transnational organized crime, and other threats to public safety? No—rather, law enforcement personnel obtain training to understand these threats, which prepares them to address the challenges when the time comes.

Similarly, law enforcement executives have to learn to address this strategic cyberthreat by obtaining cybersecurity leadership training. Today's law enforcement executives need to take cybersecurity leadership courses to understand and address the strategic, operational, and tactical aspects of the cyberthreat.

Law enforcement executives must recognize that the strategic responsibility of providing the best cybersecurity posture for their organizations lies with them. This responsibility does not fall on an agency's chief information officer (CIO), chief information security officer (CISO), chief security officer (CSO), or IT director—it falls squarely on the shoulders of the chief and senior leadership team. The CIO, CISO, CSO, or IT director play a strategic role in addressing the cybersecurity posture of the agency. But at the end of the day, who is responsible if a cyberattack destroys the agency's IT infrastructure, investigative files, evidence, and financial records? The CIO, CISO, CSO, or IT director will not be the senior executive addressing this issue with the public and the media. The chief and senior leadership team will be responsible for addressing this cyberattack and its resolution, as well as the attack's impact on the agency, its services, and the community.

Understanding the Strategic Cyberthreat: FBINA Cybersecurity Courses

Many private sector cybersecurity courses exist for cybersecurity personnel (e.g., IT staff, incident response teams, intrusion analysts, network forensic analyst, digital forensic specialists), along with cybersecurity leadership courses for CIOs, CISOs, CSOs, and IT directors. However, there are also cybersecurity leadership courses for law enforcement executives; for instance, the Federal Bureau of Investigation (FBI) offers cybersecurity leadership education to its FBI National Academy (FBINA) law enforcement executive students.

The FBINA is a 10-week professional course of study for both U.S. and international law enforcement executives nominated by their respective agencies because of their demonstrated leadership qualities. The FBINA, located at the FBI Academy in Quantico, Virginia, has had both an undergraduate and graduate Cyber Threat Landscape for Law Enforcement Executives/Leaders course since 2015. These two cybersecurity leadership courses are accredited by the University of Virginia and are designed for law enforcement executives with no cybersecurity foundational knowledge. The courses provide each FBINA student with a foundational understanding of various areas, including the following:

- Understanding the cyberthreat landscape
- Basics of information technology
- Understanding malicious software
- Computer network operations (computer network defense, exploitation, and attack) and advanced persistent threat (APT)
- Industrial control systems (ICS) and critical infrastructures
- Wireless and mobile devices and their vulnerabilities
- Web, web servers, and web exploits and vulnerabilities
- Cybercrime
- Hacktivism
- Cyber underground
- Cyber defense and liaison with IT personnel
- Incident response and digital forensics
- Cyber training and cyber certifications
- Private and public sector partnerships
- Cyber challenges for law enforcement executives

The FBINA cybersecurity leadership students learn

- to recognize the various cyberthreat actors;
- to identify the various cyber intrusion vectors impacting an organization (IT infrastructure, personnel, operations);
- to implement an enterprise-wide cybersecurity incident response (plan, personnel, training, tabletops);
- to create an enterprise-wide cybersecurity culture (cyber-savvy leadership, information security training for all employees, regular cybersecurity bulletins, advanced cybersecurity training/recruitment for cyber staff, etc.); and
- to understand the need for continuous strategic resourcing to address the ever-changing and sophisticated nature of the cyberthreat to continually maintain the organization's best cybersecurity posture (IT infrastructure, personnel, operations).

The only way this 21st-century wild frontier of global cybercrime will become more manageable is through the creation of cyber investigative teams at the state, local, tribal, territorial, and international law enforcement levels.

Upon completion, these FBINA students have become cyber-savvy law enforcement executives who understand the strategic, operational, and tactical impacts of the cyberthreat and are ready to work with their CIOs, CISOs, CSOs, or IT directors and their staff to improve the cybersecurity posture of their agencies. These newly cyber-savvy executives are also prepared to begin creating an organic cyber investigative capability.

Creating an Organic Cyber Investigative Capability

Today's private and public sectors are competing for a scarce strategic resource—cybersecurity professionals. There are not enough cybersecurity professionals to assist all private and public sector organizations in addressing the strategic cyberthreat. Due to this scarce resource, one solid solution is to create an organic cyber investigative unit of cybersecurity-trained investigators and prosecutors to address cybercrime and cyber intrusions in their respective areas of responsibility.

Many law enforcement executives have personally led efforts to create an organic investigative or law enforcement response capability during their careers. These efforts may have included creating entities such as a squad, unit, or bureau to address a newly identified threat to their community. Examples of these leadership efforts in today's law enforcement community include the creation of counterterrorism units, homeland security bureaus, active shooter response programs, and community liaison programs. These new entities use existing personnel from the law enforcement agency to address these new strategic threats with specialized capabilities. A similar process can be used to create a cyber investigative capability.

Chiefs should ask themselves if their agencies have an organic cyber investigative capability. Most cybercrime has an international nexus, and many agencies cite this as a major reason not to address cybercrime. Another reason for this lack of organic capability is the absence of cyber-savvy law enforcement leaders. If chiefs are not cyber-savvy law enforcement leaders, how do they see the response to cybercrime and cyber intrusions in their area of responsibility? Do they not address cybercrime and cyber intrusions because they believe this to be a state or federal law enforcement issue and, more important, because their agencies do not have an organic cyber investigative capability?

Cybercrime is impacting all parts of local, state, tribal, and territorial societies, from elderly individuals being scammed of their life savings by a cybercrime actor, to local businesses suffering from a business email compromise (where unauthorized wire transfers result in large losses), to the constant ransomware attacks encrypting computer systems of both private and public sector victims. The only way this 21st-century wild frontier of global cybercrime will become more manageable is through the creation of cyber investigative teams at the state, local, tribal, territorial, and international law enforcement levels. These teams can work jointly with the FBI Cyber Task Forces (FBI CTFs), the U.S. Secret Service Electronic Crimes Task Forces (USSS ECTFs), international law enforcement partners, and other investigative agencies currently addressing cybercrime and cyber intrusions.

Chiefs and senior leadership must lead the strategic effort in creating organic cyber investigative capabilities within their agencies. By championing this cause, the senior leadership will become strategic agents of change for their personnel, local communities, elected officials, and prosecutorial counterparts. An important element to having a successful organic cyber investigative capability is the support of elected officials and the local community. A successful investigative effort also requires a prosecutorial partnership. By leading these efforts, the chief and senior leadership team will ensure the prosecutor's office leadership is also cyber-savvy. In turn, agencies will receive strategic resources to create an organic cyber prosecutorial capability.

Components to Consider in Creating a Cyber Investigative Capability

A law enforcement organic cyber investigative capability requires a timeline, a multiyear budget, personnel, baseline cybersecurity training, advanced cyber investigative training, and leveraging of private and public sector cyber investigative resources.

A law enforcement organic cyber capability takes coordination and collaboration and must have a multiyear plan with the appropriate strategic resources approved and supported by the chief and senior leadership team. Developing a solid cyber investigative team requires the right personnel, with the appropriate baseline cyber investigative training, specialization with advanced cyber investigative training, and the leveraging of federal cyber investigative resources to provide the cyber unit with cyber intrusion experience.

KEY COMPONENTS FOR DEVELOPING A CYBER INVESTIGATIVE CAPABILITY

- **Financial Resources:** Cybersecurity training and equipment can be expensive; however, state, local, tribal, and territorial (SLTT) agencies can apply for cybersecurity grants to help fund their cyber investigation capabilities. In addition, many U.S. federal entities offer training and resources that might be more affordable and accessible.
- **Collaborative Resources:** Agencies who have the resources and geographical ability to assign an investigation to an FBI or a Secret Service Cyber Task Force will allow that person to gain valuable experience and knowledge that he or she can bring back to the agency. Smaller agencies or those not near a CTF can consider pooling resources to create a regional cyber investigative team.
- **Training:** Cyber team members will need baseline cyber investigate training, as well as specialized training applicable to the team members' specific roles and responsibilities (e.g., system administration, cyber defense, digital forensics, and other specializations).
- **Partnerships:** SLTTs can benefit from partnerships with public sector entities such as DHS that can provide their investigators with up-to-date cyberthreat intelligence, information sharing resources, and lessons learned, as well as training.

Financial and Collaborative Resources

The absence of a cyber investigative capability often is due to the lack of financial resources to create it. Thus, chiefs and senior leadership, as cyber-savvy leaders, should assist in making cybersecurity and the organic cyber investigative capability a strategic issue with the appropriate resources and leadership. Cybersecurity training from private sector cybersecurity vendors and the technical equipment to conduct these investigations can be expensive. Senior leadership of local, state, tribal, and territorial law enforcement agencies should direct their personnel to apply for cybersecurity grants to help create their organic cyber capabilities. In addition, cybersecurity training resources are available from federal entities, such as the U.S. Department of Homeland Security, the FBI Cyber Shield Alliance, the FBI Cyber Investigator Certification Program, the FBI Regional Computer Forensic Laboratory, the USSS National Computer Forensics Institute, and the National White Collar Crime Center (NW3C).

To create an organic cyber investigative capability, agencies should leverage the various federal cyber investigative resources, such as the FBI CTFs and USSS ECTFs. The FBI CTFs are located in each of the 56 FBI field offices across the United States, and USSS ECTFs are located in numerous cities across the United States. Chiefs and senior leadership should consider assigning an investigator as a federal task force officer (TFO) to either of these cyber investigative task forces. Having a TFO assigned to a cyber investigative task force will provide him or her with cybersecurity training, valuable cyber investigative experience, and the knowledge of how a cyber investigative task force operates. State, local, tribal, or territorial law enforcement agencies who assign their personnel as FBI CTF or USSS ECTF TFOs can then use this cyber investigative knowledge to assist in creating their own organic cyber capability.

For the state, local, tribal, and territorial law enforcement agencies not located near an FBI field office or USSS ECTF location, chiefs should consider pooling investigative resources in their area of responsibilities and create a county or regional cyber investigative task force. By doing so, each contributing agency would have a cyber investigative resource to utilize in their respective jurisdictions.

Training

Another component in creating an organic cyber investigative capability is to provide selected personnel with baseline training, which could include such courses and cybersecurity certifications as CompTIA A+, Network+, and Security+ certifications. Baseline cyber investigative courses include the NW3C two-day CC 101 Basic Digital Forensic Imaging Course and the NW3C four-day CS 235 Basic Network Intrusion Investigations Course.

Once baseline cybersecurity training is provided, the cyber team leader must select specialization training for the cyber investigative team personnel. The chief and senior leadership team need to understand these advanced cybersecurity training courses can be very expensive. The cost for one advanced cybersecurity course could include the cost of the cybersecurity class; the cybersecurity certification exam; and travel, hotel, and per diem for each of their cyber investigative team members. The chief and senior leadership team should ensure each team member who takes a cybersecurity course successfully passes any accompanying cybersecurity certification. By doing so, each team member will receive cybersecurity credentials respected in the cybersecurity community, and this requirement will ensure the cyber team member studies and successfully learns the course objectives.

U.S. FEDERAL TRAINING RESOURCES

- DHS National Initiative for Cybersecurity Careers and Studies (NICCS): https://niccs.us-cert.gov
- DHS Industrial Control Systems Cyber Emergency Response Team (ICS-CERT): https://ics-cert.us-cert.gov
- National White Collar Crime Center (NW3C): www.nw3c.org
- U.S. Secret Service, National Computer Forensics Institute (NCFI): www.ncfi.usss.gov/ncfi
- FBI Cyber Investigation Certification Program (CICP): www.cjis.gov (accessible via LEEP)

There are numerous types of advanced cybersecurity specializations, including the following areas:

- System Administration (such as Windows, Unix, Mac OS)
- Cyber Defense (Intrusion Detection, Security Windows/Linux/Mac OS, Active Defense)
- Digital Forensics (Advanced Smartphone Forensics, Memory Forensics, Advanced Incident Response)
- Intrusion Analysis (Intrusion Analysis, Network Digital Forensics)
- Industrial Control Systems (Fundamentals of ICS, ICS Incident Response)
- Penetration Testing (Network, Mobile, Web, Wireless, and ICS Penetration Testing)

Additional areas of advanced cyber investigative training include management, legal, and audit. Several private sector cybersecurity vendors such as SANS, ISC^2, Offensive Security, EC-Council, CompTIA, ISACA, and Cisco provide basic, intermediate, and advanced cybersecurity training to law enforcement and private sector cybersecurity personnel.

Partnerships

An organic cyber investigative capability offers the ability to create invaluable partnerships with both private and public sector entities. U.S. state, local, tribal, and territorial law enforcement agencies need to partner with such public sector entities as the U.S. Department of Homeland Security (DHS). The DHS National Cybersecurity and Communications Integration Center (NCCIC) is a 24/7 cyber situational awareness, cyber incident response, and management center that is a national nexus of cyber and communications integration for the U.S. federal government, the U.S. intelligence community, and U.S. law enforcement. DHS can provide state, local, tribal, and territorial law enforcement agencies with the most current cyberthreat intelligence to assist their organic cyber team capabilities. DHS NCCIC branches include the U.S. Computer Emergency Readiness Team (US-CERT), Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), the NCCIC Operations and Integration branch, and the National Coordinating Center for Communications (NCC). DHS also sponsors multiple cyber information sharing entities and works closely with the various critical infrastructure sectors information sharing and analysis centers (ISACs), such as the Multi-State ISAC (MS-ISAC). The MS-ISAC is designated by DHS as the cybersecurity ISAC for state, local, tribal, and territorial governments. In addition, multiple public sector entities can provide cybersecurity intelligence, such as the FBI's Internet Crime Complaint Center (IC3), the FBI Cyber Shield Alliance, and the IACP's Law Enforcement Cyber Center.

Chiefs and their senior leadership teams understand the importance of good community relations. Likewise, it is no different when creating cybersecurity partnerships with state, local, tribal, and territorial private sector partners. Creating cybersecurity partnerships with local private sector partners can assist state, local, tribal, and territorial law enforcement agencies' overall cyber investigative and cyber intelligence capabilities. Private sector partners can share local cyberthreat intelligence, lessons learned from local cybersecurity incidents, participate in local joint cyber incident tabletop exercises, and provide free cybersecurity training.

Conclusion

Today's law enforcement profession must strategically, operationally, and tactically address the strategic cyberthreat. Law enforcement agencies' senior, mid-management, and first-line leaders need to be cyber-savvy. Agencies should strategically create a cybersecurity culture that envelops the entire agency and its employees. Such leadership will incorporate the cyberthreat in proper strategic planning and resourcing resulting in properly defending the agency's IT infrastructure, personnel, and operations.

Agencies should create an organic cyber investigative capability in their area of responsibility. Such capability should involve identifying financial and collaborative resources, available training, and grants. Law enforcement executives, who establish an organic cyber investigative capability, will ensure their communities are protected from the various cyberthreat actors currently harming their residents. ❖

Accident Support Services International Ltd.

Bulletin.

ACCIDENT SUPPORT SERVICES INTERNATIONAL LTD.

Issue 04

Arizona's First Collision Reporting Center!

Tucson Arizona is the 33rd largest city in the United States. At 236 square miles, surrounded by five mountain ranges and located in the Sonoran Desert, the only place that the ancient and majestic Saguaro Cactus grows, the city is home to 540,000 people.

Tucson is also the home of Arizona's first Collision Reporting Center, the second CRC in all of the United States. Tucson Accident Support Services Ltd. is pleased to partner with the Tucson Police Department to open our newest CRC at 1100 S. Alvernon Way, Tucson in May of 2018.

The Tucson Police Department was founded in 1871 with a single Marshall. Today, over 830 sworn officers and 300 civilian staff members serve this law enforcement agency and community. The mission of the Tucson Police Department is to serve the public in partnership with their community, to protect life and property, prevent crime and resolve problems.

The Tucson Collision Reporting Center is a partnership between the police, insurance industry and Accident Support Services International Ltd. (ASSI). Collision reporting services are provided at No Cost to the Police or the public; they are paid for by participating insurance carriers. Through their partnership with ASSI in the Collision Reporting Center, Tucson Police will have the opportunity to divert simple property damage collisions with no major injuries or criminal aspect to the CRC and reallocate more officers to higher priority calls for service and crime prevention programs. Analysis of the Tucson collision data collected by ASSI in our Collision Reporting and Occurrence Management System (CROMS) will assist the Tucson Police to develop more pro-active road safety programs to prevent accidents.

Establishment of the Tucson Collision Reporting Center also allows the Tucson Police Department to enhance their already excellent service to the public, enabling involved drivers to complete their collision reports in a safe and comfortable environment with empathetic CRC staff to assist them in the reporting process and reach out to their families and their insurance companies for next steps.

Insurance Carriers in the southwest will benefit from First Notice of Loss as their policy holders are still reporting at the CRC; increasing their customer service opportunities with immediate tow, vehicle repair and replacement vehicle rental recommendations. Placement of our "Damage Reported to Police" stickers on the vehicles, along with photographs of the damage taken by the CRC also assist insurers to quickly determine possible insurance fraud.

ASSI looks forward to working together with the Tucson Police Department, partner insurance carriers and the citizens of Tucson at the Tucson Collison Reporting Center to provide our one-stop collision reporting program solutions, simplifying the collision reporting process for everyone.

This Issue:

ASSI Innovation, Exceptional Customer Service, On the Road

ASSI - Accident Support Services INNOVATION

Accident Support Services hosts regular User Group Meetings, Insurance Advisory Council gatherings and operational review meetings with our individual insurance industry partners. The purpose of these meetings is not simply to bring ASSI information to our insurers, but to discover how our company may modify or improve our programs to bring added value to the insurance claims process.

ASSI is proud to be working with a major insurance carrier in North America to accept the collision data gathered at our Collision Reporting Center to populate their First Notice of Loss (FNOL) claims module. The concept will have data in real-time transferred to the carrier's system to confirm by policy number the insured's information and whether a claim is active at the time of receipt. If this is a new claim, then the system will accept the information and return a claim number which CRC staff will provide to the insurer's policy holder during the interview process at our Collision Reporting Center.

We have also completed testing with a new on-line insurance start-up company which will receive all of its information electronically from FNOL to invoicing of reporting packages. Accident

Support Services has been able to successfully accommodate and link with this company to populate their claims system and return a claim number to our CRC counselors to provide to the policy holder while still in our Center.

With FNOL integration, one size does not fill all! ASSI will continue to work with each of our insurance partners to create solutions that will enable each carrier to provide early intervention and the best customer service to their customers.

Travelling the "Road to Zero" ASSI supports Road Safety Efforts

Accident Support Services is a proud supporter and contributor to the Road to Zero Campaign in every jurisdiction we service. We work with local government and road safety professionals in providing important and timely data for engineering departments to analyze and review to improve road conditions and save lives.

A recent Release from the U.S. Department of Transportation discusses the Road to Zero launched in 2016 in response to increasing traffic fatalities across the nation. The 2015 year had posted the largest increase in traffic deaths since 1966 and preliminary statistics for 2016 were projecting another alarming uptick in fatalities - an increase of about 10.4 percent as compared to the number of fatalities in the first half of 2015.

Anthony Foxx, US Transportation Secretary was quoted, "Our vision is simple – zero fatalities on our roads. We know that setting the bar for safety to the highest possible standard requires commitment from everyone to think differently about safety– from drivers to industry, safety organizations and government at all levels."

The Release continues, "Every single death on our roadways is a tragedy," said NHTSA Administrator Mark Rosekind. "We can prevent them. Our drive toward zero deaths is more than just a worthy goal. It is the only acceptable goal."

As providers of critical and timely automotive accident report data for each jurisdiction we work with, Accident Support Services International is doing our part to make a difference and assist in the campaign to achieve a "Road to Zero".

Did you know?

During our interview process with your policyholder we ask every person if they have contacted their insurance provider yet? What we found was very interesting and supports the need for integration with our insurance partners. ASSI found that over 65% of policyholders had not contacted their insurance company before coming to the Collision Reporting Center. As we all know, one of the biggest complaints from claimants is that they have to repeat themselves in multiple situations when dealing with their claim.

With the knowledge that we handle over 60% of your policyholders before you hear about the claim provides a unique opportunity to improve customer experience and reduce administrative expenses in setting up a claim.

At ASSI, we are prepared to work with our partners to facilitate a transfer of information to create a First Notice Of Loss transfer. Not only can we assist with populating your claims file but we can also work with you to provide an informative brochure/instruction on what the next steps are before they leave the CRC.

Imagine your claims adjusters being able to pro-actively contact your policyholder and confirming the accident and where they have taken their vehicle and know if there were any injuries at all. Your policyholder will be happy that their insured is calling to make sure they are OK and handle any questions they may have.

Also consider that all pictures can now be transferred to your appraisal supplier to create the estimate to be sent over to the shop to prepare for and schedule the work into the facility. All of this can help save time and money for every insurer.

Contact Rick Yates at ryates@accsupport.com to discuss the opportunities available to our insurance partners!

ASSI - Finalist in ICTA 2018

The ICTA, Insurance Canada Technology Awards, were recently presented at the Insurance-Canada.ca Technology conference. These awards highlight and celebrate the use of technology impacting insurance processes. Accident Support Services International Ltd. is pleased to have been a finalist this year, part of a field of distinguished nominees.

ASSI was nominated for enhancements to our Collision Reporting and Occurrence Management System (CROMS) that include our Damage Estimator Tool and Citizen Photograph Upload Feature.

The Damage Estimator or appraisal tool provides insurers with a more accurate and consistent record of expected repair costs from information entered and calculated at the Collision Reporting Center (CRC), allowing adjusters to be vigilant in cases where actual repair invoices may vary disproportionately. This tool includes a Total Loss calculator that will notify insurers and enable them to take immediate action with a vehicle where weighted rankings on the CRC questionnaire identify a potential total loss. This is designed to reduce the average settlement time of total loss vehicles by up to 20%.

(l-r) Rob Martin, Director of Sales, Octo Telematics (Award Sponsor), Lynn Hemingway, Vice President Operations, Accident Support Services International Ltd., Andrew Lo, President and CEO, Kanetix Ltd. (Award Sponsor)

Another new feature included as part of this nomination is the Citizen Photo Upload tool. Drivers involved in collisions now have the opportunity to provide their personal photographs of the damage to be included as part of their collision report file. Drivers are notified of this option when they report at the CRC, and they may upload immediately or later from the comfort of their home or office. Insurers have access to all uploaded photographs for both their insured or any third party involved in the collision, to assist in fault determination and in identifying possible additional damage when compared to damage photographs taken by CRC staff.

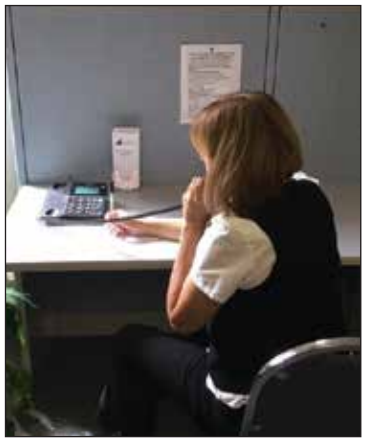
Our insurance partners are currently enjoying the benefits of these enhancements in their claims process.

Accident Support Services International Ltd. was the recipient of a 2013 ICTA award for our CROMS program.

CROMS is also the recipient of the 2005 Microsoft Impact Award for Integrated E Business Solution of the year and a finalist for the 2008 Microsoft Impact Award for Custom Development Solution of the Year.

Imagine Exceptional Customer Service

Just imagine. What a day! You've been involved in an accident. Thankfully, no one has been seriously hurt. You exchange pertinent information with the other driver: plate, driver license, name, address, insurance particulars. You call the Police to make a report and are directed to your local Collision Reporting Center (CRC). You attend at the CRC and the Accident Support Services counselor assists you in making your collision report, photographs your damaged vehicle, advising you on next steps including contacting your insurance company. Now what? How long is your insurance claim going to take? How will you get your car repaired? Is this all going to be a circle of telephone tag, inconvenience, time and trouble?



Now imagine this. Your insurance company has an office right inside the CRC where you reported your collision. The ASSI Counselor introduces you to a Claims Adjuster from your insurance carrier who will immediately initiate your collision claim, provide information on car rental and repair options so you don't have to search the internet, and help you get back to your regular routine with much less stress and worry. As a driver, you are more than pleased to have such amazing customer care and service when you really need it.

It is not your imagination! Allstate Insurance currently occupies a customer care office in one of our Collision Reporting Centers. TD Insurance will move into another CRC in April. A third facility will welcome insurer customer care offices later this year. Benefits to the insurer include immediate personal contact with policy holders to assist in mitigating further tow, rental and repair costs. As well, the opportunity to provide your exceptional on-the-spot customer service to reporting drivers will certainly result in increased customer satisfaction and retention.

For more information on imagining your own customer care space in one of our CRCs, please contact VP Rick Yates at ryates@accsupport.com

Tucson Insurer Information Sessions

ASSI Vice Presidents Rick Yates and Lynn Hemingway recently met with local Tucson insurers to present information and answer questions on the upcoming Tucson Collision Reporting Center (CRC) and the resulting changes to collision reporting for their policy holders.

Drivers involved in collisions will be directed by Police to attend the new Tucson CRC to complete their collision reports. Our empathetic staff will interview the reporting drivers in our safe and comfortable location at 1100 S. Alvernon Way, assisting them to complete their required collision reports. Our staff will photograph the vehicle damage and place a "Damage Reported to Police" Sticker on the vehicle that serves as a warning to body shops that damage has been recorded, in an effort to thwart possible insurance fraud. Participating insurers will receive notification of the collision report, often while their policy holder is still at the police station.

By providing insurers with all relevant facts of the loss (first notice of loss) including documentation and photographs of all parties within hours of the collision as they are reporting to police, ASSI helps reduce claim cycle times and related costs. Our program helps to increase penetration of carriers' preferred appraisal resources, improve customer service, and reduce the likelihood of physical damage and bodily injury fraud, while enabling insurers to significantly improve claim outcomes and policyholder retention by streamlining the claims reporting and settlement process.

It was our pleasure to meet insurers in Tucson to discuss our collision reporting programs and the benefits to insurers, police and the public. We are looking forward to working together in Tucson.

Rick Yates, VP Insurance programs leads Tucson Insurers information session on Tucson Collision Reporting Center.

On the Road with ASSI

The Accident Support Services International Team will be on the road this season at the following events:

June 17 – 21 – AAMVA, Region 2, Myrtle Beach, SC
June 24- 27 – Michigan Association of Chiefs of Police (MACP), Bellaire, MI
June 25-27 – America's Claims Event, ACE, Austin, TX
August 8 – 10 – NACE Conference, Atlanta, GA
August 21 – 23 – AAMVA International, Philadelphia, PA
August 26 – 29 – GHSA, Atlanta, GA
September 9 – 11 – IASIU Conference, Baltimore, MD
September 9 – 12 – Virginia Association of Chiefs of Police Conference, Roanoke, VA
October 21 – 24 – IACP Conference, Orlando, FL
October 28 – 30 – PCI Annual Conference, Miami, FL.
October 31 – Nov. 2 – SEMA, Las Vegas, NV

We look forward to meeting with you to discuss our Collision Reporting Center and Collision Reporting and Occurrence Maintenance System (CROMS) programs.

CCIDENT SUPPORT SERVICES INTERNATIONAL LTD.
631 Abney Road, Roanoke Virginia 24012-1257
Toll Free: 1-877-895-9111
For more information, go to www.accsupport.com
Recommendations, Suggestions, Comments, contact:
Editor: Jane Ross admin@accsupport.com

Myths and Realities of Going Dark:

Talking Points for SLTT LE Executives

By Rich Littlehale, Special Agent in Charge, Technical Services Unit, Tennessee Bureau of Investigation; Thomas Ruocco, Division Director for Criminal Investigations, Texas Department of Public Safety, Chair, IACP Police Investigative Operations Committee; Jim Emerson, Lieutenant Colonel (Ret.), U.S. Marine Corps, Chair, IACP Computer Crime and Digital Evidence Committee

Investigators are in a fight in the offices and cubicles of any law enforcement agency… one where the other side is gradually getting the better of them. Any subscriber to a technical law enforcement listserv can watch it happen in real time—ICAC (Internet Crimes Against Children Task Force) investigators, the folks who run wiretap systems, and cyber investigators will see a steady stream of questions and complaints. "Anyone have a real person I can call at Company A? They just kicked back my search warrant without any explanation, and no one is answering my emails." Or "Anyone know what kind of evidence I can get from WhatsApp? My wiretap target just switched over from phone calls." It goes on every day, and these days, law enforcement calls it "Going Dark."

The challenge is gathering digital evidence at a time when the marketplace and technical innovation have combined to create a hostile environment in which government is seen as just another potential adversary and systems are designed to protect user privacy at all costs—including from law enforcement. As one would expect, these struggles are felt particularly acutely in cybercrime and cyber-enabled crime investigations, because a higher percentage of the evidence in those cases exists in the digital world. Going Dark affects a wide and growing range of cases because digital evidence is relevant to a wide and growing range of cases.

This has been a thorny problem for a while now, but just as there are unprecedented challenges, there can be unprecedented opportunities. Even a casual observer will notice that legislators and consumers are starting to question the absolute faith they put in technology companies. This is not because the companies are inherently lawless or evil, but just because they are companies like any other and probably should be subject to regulation for the common good like other companies. IACP recognizes the challenges and the opportunities and is considering the formation of a multi-committee working group to coordinate messaging on Going Dark and efforts to mitigate its impact.

The message is simple—investigators of state, local, tribal, and territorial (SLTT) agencies are in a fight, and they need their executives' help. Federal partners have taken the lead on messaging in this area, but they can't get the ball over the line without the help of SLTT leaders; agencies must demonstrate to policymakers that this is a problem for all of law enforcement. Some of the obstacles involve resources and training, yes, but progress is also linked to authorities and advocacy. The talking points presented herein will prepare SLTT executives to engage on this topic when they have the chance, adding their voices to the growing chorus that something has to change—and that the rule of law can't be subordinated to the whims of any one industry, however powerful. While some of the points referenced are based on U.S. law, Going Dark is a global issue, and many of the talking points are relevant to law enforcement worldwide.

Talking Points

- SLTT law enforcement agencies conduct the majority of criminal investigations and prosecutions, and they are a diverse group with a wide range of capabilities and needs; the Going Dark set of access to digital evidence challenges affect them all in different ways, but it is a problem for everyone, not just federal agencies.
- These problems are felt particularly strongly in cybercrime and cyber-enabled crime investigations because most of the evidence in those cases is digital.
- Access challenges to digital evidence like encryption are having real impacts on critical SLTT law enforcement investigations every day, and often they are obstacles to investigations in the most serious cases of human trafficking, homicide, kidnapping, and online crimes against children.

Myth #1—Going Dark Is Just About Encryption

Going Dark got its start as a reference to the gradual loss of access to evidentiary communications because of encryption, but it has grown to encompass a range of access to digital evidence challenges. One often hears the term "the golden age of surveillance" when technology and privacy advocates respond to investigators' cries for help: "What's the problem? There is 'digital dust' behind every corner, just waiting to be gathered." The truth is that everywhere law enforcement turns, investigators are running into problems gathering digital evidence, and encryption is only one of them. "Digital dust"—a catch-all term like "metadata" used to refer to the myriad details created by connected devices short of actual content evidence—will get an investigator only so far. In criminal court cases, content is king, and law enforcement is steadily losing access to more and more content evidence.

Talking Points

- "Going Dark" isn't just about encryption—it involves a range of barriers to accessing digital evidence.

- Tech companies create obstacles like the Microsoft Ireland foreign evidence problem by designing their networks without any thought to the impacts on public safety and then refusing to comply with legal demands until the law is changed to require them to do so, such as with the recent CLOUD Act.[1]
- There must be legal structure around response times to legal demands for evidence from service providers; the law provides no guidance here, and, in routine cases, turnaround times can stretch into months.
- Currently under the Electronic Communications Privacy Act, the companies control whether or not a particular law enforcement request is an emergency—so a tech employee, not a law enforcement professional with access to case facts, controls whether evidence will be produced.[2] That is a fundamental and harmful change to the U.S. constitutional principle that law enforcement controls exigency decisions and then must justify them in court after the fact.
- It isn't really the "golden age of surveillance" when every time investigators ask for something, they're told no, whether its encrypted content, evidence stored overseas, evidence the companies don't want to admit they are collecting, or evidence that they intentionally don't retain.

Myth #2—Going Dark Can Be Solved Without Regulating Encryption

This is a quick point, but a very necessary one to consider nonetheless. The rogue's gallery of digital evidence challenges above are cited by some as a reason why the need to regulate encryption isn't the right question. "Let's fix all these other things first," goes the argument, along with suggestions to provide law enforcement with a lot more training and resources… and then see whether encryption is still a problem.

There are two main problems with that line of reasoning: First, there doesn't seem to be much of a drive to fix any of these other problems, so this argument can be fairly seen as an attempt to distract from the encryption question without a sincere intent of meaningful changes. Second, simply because a series of measures might help, that doesn't mean that they are the socially optimal solution to the problem. Look at lawful hacking as an example: lawful hacking advocates argue that, instead of regulating encryption, the field should increase resources for law enforcement to break into devices without the consent or cooperation of the companies. Private companies that engaged in an arms race with Apple and Android to crack encrypted smartphones are probably the best example of these "resources." That approach may get law enforcement investigators some of the evidence they need some of the time, but only at great expense and only on a limited scale. In addition, the government will face increased pressure to share the necessary exploits (hacks) with the companies in order to secure their products against other attackers like hostile governments, rendering solutions short-lived.

A balanced system that permits exceptional access across widely used devices and networks is a far more rational, socially preferable solution. ("Exceptional access" refers to a mechanism to access decrypted content in response to legal demands.)

Talking Points

- The substitutes for encrypted content that are sometimes offered, like increased use of metadata or more investment in "lawful hacking" tools, aren't nearly as effective as they're made out to be, especially in court.
- Unlike the intelligence community, state and local law enforcement must prove their case beyond a reasonable doubt in a court of law—metadata and "digital dust" just don't get the prosecution over the finish line much of the time.
- Alternatives like "lawful hacking" aren't real alternatives, and they have many problems of their own—they don't scale, they are expensive, and they pit government in an arms race against industry. That isn't a socially optimal solution to the problem.

Myth #3—An Exceptional Access Mandate Is Technologically Impossible

A recent round of reports on this topic makes two things clear: (1) exceptional access to encrypted evidence is a policy question, not a technology question, and (2) in order to have an honest conversation about exceptional access, everyone will have to abandon entrenched positions.[3] All too often, opponents of exceptional access to encrypted evidence say, "it can't be done," when they mean, "we are afraid of where an honest conversation will lead." A law that requires mass-market service providers to maintain the ability to decrypt content in response to proper legal demands is consistent with long-standing tradeoffs between theoretically absolute security and the social usefulness of the system.

Talking Points

- Law enforcement understands that exceptional access can be a system requirement just like any other and that establishing this access triggers tradeoffs that are similar to other tradeoffs made for business purposes all the time. It is denying a technological reality to say that a system requirement for exceptional access is technologically impossible or even commercially impractical. It is already happening in deployed systems all the time.
- The status quo grants the average user absolute and unprecedented power to keep secrets from the government, even where there is a compelling public safety reason, with appropriate judicial oversight, to gain access to those secrets. It is for this reason that this is a policy issue, not a technology issue.
- The current state of affairs is that companies are willing to trade that absolute privacy so as to be granted access to customers in repressive regimes, but they withhold that public safety benefit from citizens in free societies.
- Exceptional access can be implemented without fundamental changes in the trust relationship that currently exists between users and service providers.
- An exceptional access mandate doesn't have to grant 100 percent access all of the time to be useful. Targeting widely distributed devices and networks with millions of users will help a great deal.
- Companies already implement features that look like exceptional access all the time without unacceptable problems. They maintain signing keys for software updates, give the encryption keys to their cloud platforms to third parties for storage, and maintain last-ditch data decryption mechanisms in case of litigation.
- Exceptional access is consistent with long-standing tradeoffs between theoretically maximal security and usability—this simply adds government access as a system requirement.

Myth #4—There's Nothing SLTT Law Enforcement Can Do About Going Dark

When faced with a problem of the technical and policy complexity of Going Dark, it is tempting for SLTT law enforcement to throw up their hands and say, "I'll leave that to the feds." But the reality is that the IACP committees with a stake in this—and their sister committees in other law enforcement organizations—are involved in an ongoing fight on multiple fronts, and they need the help of all law enforcement agencies, regardless of size or jurisdiction. There is an

ongoing dialogue with policymakers in Washington, DC, about how regulation can help with encryption and other Going Dark challenges. In order to sustain and grow that effort, SLTT agency leaders must step forward as advocates and encourage their investigators to provide cases and examples of problems to the National Domestic Communications Assistance Center to catalog this problem.

In addition, working with prosecutors to pursue show cause hearings when providers obstruct access to digital evidence and finding ways to increase resources and training available to investigators working the digital crime scene are additional ways that SLTT law enforcement executives can help combat this issue.

The Going Dark challenges around access to digital evidence are a fact of life for investigators working the digital crime scene in 2018. And just as cybercrime and cyber-enabled crime touch a large and growing percentage of all criminal investigations, Going Dark is hurting investigators' ability to gather the evidence they need to do their jobs more and more every day. SLTT law enforcement executives have an opportunity to mitigate this harm by educating themselves, pursuing training and resources, and adding their voices to those of federal partners in advocating for legal help for investigators. The effort to create a working group on this issue within the IACP committee structure is an important step to meeting this growing challenge.

Talking Points

- SLTT agency leaders take as a starting point the fact that there is an expectation (and need) for every player involved in the criminal justice system to abide by the same roles—including companies in possession of evidence—therefore, a legal demand should be respected by a technology company just like it is by everyone else.
- Going Dark is not an effort by law enforcement to demonize big tech; however, neither should these companies be given a pass. They have a tremendous amount of wealth and power, and they should be expected to play by the same rules that everyone else does.

Conclusion

The current impasse leaves law enforcement and technology companies eyeing each other at a distance over a wide gulf of rhetoric and platitudes. It is understood that it is very difficult to build stable, secure international communications networks, but it is also hard to keep people safe from crime and terrorism in a free society. That's why an open and honest dialogue about options and tradeoffs is very important right now—one that includes regulation of encryption and the other digital evidence challenges, the exploration of resourcing problems and solutions, training opportunities, and all the other issues that are making it difficult to work the digital crime scene of the 21st century. Going Dark is a real problem, and it is going to take real effort across the whole range of stakeholders to fix it. ❖

Notes:

[1]Devin Coldewey, "Supreme Court Dismisses Warrant Case Against Microsoft After CLOUD Act Renders It Moot," TechCrunch, April 17, 2018.

[2]Electronic Communications Privacy Act of 1986, 18 U.S.C. §2510-22.

[3]National Academies of Sciences, Engineering, and Medicine, *Decrypting the Encryption Debate: A Framework for Decision Makers* (Washington, DC: National Academies Press, 2018); EastWest Institute, *Encryption Policy in Democratic Regimes: Finding Convergent Paths and Balanced Solutions* (New York, NY: EastWest Institute, 2018), https://www.eastwest.ngo/sites/default/files/ewi-encryption-us-version.pdf.

Management and Leadership
Highway Safety
Crime Scene and Forensic Science
Police Motorcycle
Community-Police Partnerships

Every Dimension of Public Safety

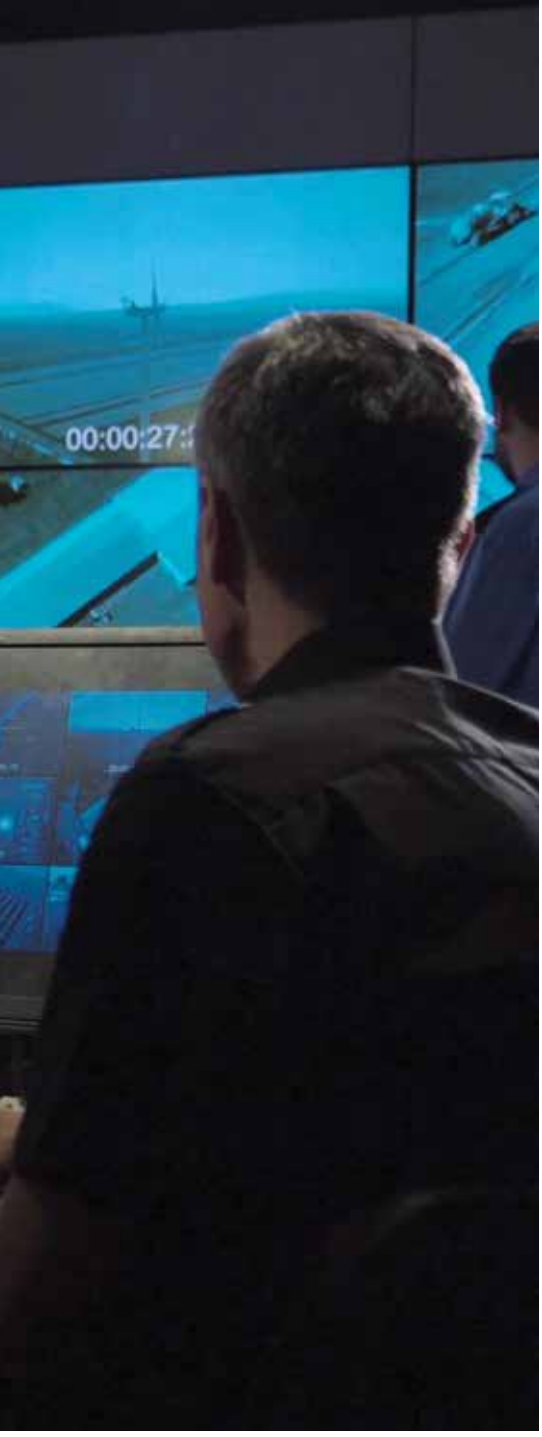
Only at Northwestern.
More than 50 courses providing professional skills with a leadership perspective. On campus, around the country and online.

Find the right course for your department.
nucps@northwestern.edu
or 800-323-4011

Northwestern | CENTER FOR PUBLIC SAFETY
nucps.northwestern.edu

Starting a Forensic Video Unit: What Chiefs Need to Know

By Brandon Epstein, Sergeant, New Brunswick, New Jersey, Police Department



Many agencies across the world have realized the increasing importance of digital evidence in criminal investigations. Video evidence has been particularly useful not only in solving crimes, but in illustrating events to a jury, as well. Video evidence can often be the deciding factor in a jury's determination of innocence or guilt, with questions like "Where is the DNA?" being replaced with "What does the video show?"

Although it is widely accepted that video evidence plays a significant role in many—perhaps even most—major investigations, a dedicated team (or even a single staff member) to acquire, process, analyze, and interpret video imagery is uncommon at law enforcement agencies. As agencies begin to realize the benefits of using the full power of video evidence, they are faced with the task of creating new units without much guidance on where to begin. Having dealt with that very same challenge, the author offers his lessons learned, recommendations, and important considerations for starting a forensic video unit.

The eventual success of any video forensics unit first depends on the mind-sets of those creating it. Forensic video analysis is a recognized forensic science (a subspecialty within forensic imaging) and should be treated as such.[1] Agencies who understand that video analysis is a forensic science that employs a computer as a tool rather than an IT function that works with video are tremendously more successful, as they are run accordingly and the staff better understand their roles.

Among the initial considerations to be made when starting a video forensic unit are the capabilities and functions the unit is intended to perform. Those goals can help dictate factors such as the staffing, training, hardware, and software necessary to get started. Some video evidence units are tasked solely with retrieval of video evidence from crime scenes and field locations. This practice helps ensure that evidence is collected properly while freeing up investigative personnel for other tasks. Other units might process the collected video evidence to allow for easy playback by investigative personnel, generate still images for dissemination, and perform image enhancement. The most advanced video evidence units will perform full analysis of video imagery and generate opinions for use in court. They will be able to articulate that a specific object appears the same (or different) in recorded video as compared to real life, as well as scientifically demonstrate or explain why. This is the true science and expertise involved in forensic video analysis.

Unit Staffing

One of the most critical and difficult decisions to be made in the creation of any video forensics unit is the selection of staff assigned to it. There is no specific single formula for success, but, like in many other aspects of law enforcement, the right person for the job can be the difference between success and failure. For some agencies, this step might entail an initial decision of using sworn or civilian personnel for the role; each group comes with its own strengths and weaknesses.

Sworn law enforcement personnel have been used to perform forensic roles for many years in police agencies, and forensic video analysis is no different. A law enforcement officer is comfortable with handling evidence, writing reports, testifying in court, and working within a police agency structure. Since forensic video analysis is not a widely recognized field when entering police service, agencies may have difficulty identifying personnel with the computer skills or interest in learning about video forensics.

Civilian personnel with a background in communications or video production and editing can bring core subject matter knowledge to a forensic video unit position. Additional training in forensic video skills, as well as police procedures, would be necessary before taking on any casework. Writing reports and courtroom testimony may be completely foreign to new civilian staff and would require additional training as well.

Staff retention is a real concern in a video forensics unit; training is not a short process, and experience is necessary to become truly proficient. While sworn personnel often spend an entire career in one police agency, civilian staff may receive training and gain experience simply to leave for the private sector. Even with career law enforcement officers, it is not uncommon for a sworn forensic analyst to become fully trained and competent in the job functions, just to be promoted or transferred out of the unit. Care must be taken in selecting the right people for the job and developing strategies to retain them within the unit. This can include budgeting for supervisory roles in the future or performing a market survey of comparable salary and benefits in the field to remain competitive.

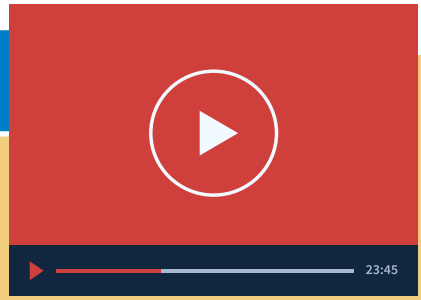
Training

Like Rome, forensic video units are not built in a day. Understanding the manner in which digital video is recorded and stored, as well as learning to process and analyze video, takes a considerable amount of time and dedication. Training classes are often highly technical in nature, introducing various math and computer science principles. Computer competency before even stepping foot in the door is a must, as courses will typically combine classroom concepts with practical applications in a lab environment.

In addition to the intense training itself, the available courses are held only a few times per year, and staff often has to travel to attend a course. Agencies must be prepared for cost and logistics of not only the training, but also the travel involved. Costs may be mitigated by hosting a course at the agency, but the agency then must assume the responsibilities that come along with hosting. It is also unrealistic to think that personnel may attend one training class and return an expert on all things video; multiple weeks of training are necessary to become proficient. (See sidebar on page 44 for examples of training options offered.)

Aside from the initial training associated with gaining proficiency in video forensics, a considerable amount of continuing education is necessary. Since video is a quickly evolving technology, there is always a new

FORENSIC VIDEO TRAINING



Law Enforcement and Emergency Services Video Association International

The Law Enforcement and Emergency Services Video Association International (LEVA) offers a significant amount of training in video forensics. A nonprofit corporation, LEVA provides training and certification in forensic video analysis around the world. At the core of LEVA's training curriculum are four, one-week courses on many aspects of forensic video analysis. The courses are held anywhere from one to four times a year in various locations; typical costs for law enforcement are $1,000 to $1,675, dependent on the specific class.

After the successful completion of the first two courses, participants can earn certification as a Certified Forensic Video Technician (CFVT), which is for personnel who process video evidence and perform video enhancement, but do not perform full analysis. After successful completion of all four core courses and some additional requirements, personnel may earn LEVA certification as a Certified Forensic Video Analyst (CFVA). This certification is for personnel who perform full video analysis and give opinion testimony in court; it is not easy to obtain and takes a considerable amount of time and effort from the candidate, as well as support from the responsible agency. By comparison, there are currently more than 300 CFVTs, but less than 60 CFVAs in the world.*

The International Association for Identification

The International Association for Identification (IAI) also maintains a forensic video certification board and presents material on forensic video evidence at its annual conference. Aside from LEVA, the IAI Certified Forensic Video Examiner (CFVE) is the only other widely recognized certification in the forensic video field.†

The Federal Law Enforcement Training Centers

The Federal Law Enforcement Training Centers (FLETC) offers a five-day basic video acquisition course titled "Recovery of Video from CCTV Video Recording (RECVR)" at its Glynco, Georgia, location. The RECVR course concentrates on the retrieval of video evidence from digital video recorders as well as playback of that acquired evidence. There is a cost associated with the RECVR training (over $2,000); however, it does include a laptop computer as well as hardware and software for the participants to take back to their agencies. There may be limited subsidies available on an annual basis for state and local law enforcement to cover the cost of training.‡

Vendor-Specific Training

In addition to dedicated training providers, there are quite a few vendors that offer specific training on their commercial hardware or software applications for use in forensic video analysis. This training is essential for effectively using the product, but it should not be considered a substitute for a basic understanding of forensic video concepts and principles. Most often, vendor training is to give the participant knowledge and proficiency in a specific tool; it does not always address the underlying reasons of why the tool is used or how it works. This information may be essential for the tool's proper use in casework as well as introducing evidence in court. There is no "magic button" in video forensics, and agencies should be wary of any commercial claims that a software package and one week's worth of training will produce a fully capable forensic video expert.

Notes:

* Law Enforcement & Emergency Services Video Association International, Inc. (website), www.leva.org.
† International Association for Identification, "Forensic Video Certification," www.theiai.org/certifications/video.
‡ Federal Law Enforcement Training Centers, "Recovery of Evidence from CCTV Video Recording," www.fletc.gov/training-program/recovery-evidence-cctv-video-recording.

concept, tool, or technique on the horizon. Staff must have the time to do online research on emerging trends, as well as the ability to attend conferences and training to stay current. The Law Enforcement and Emergency Services Video Association's annual training symposium and the International Association for Identification's annual conference are the most popular educational forums for maintaining video analysis proficiency.

Computer Hardware

As in every law enforcement unit, personnel must be given the right tools for the job. In video forensics, this involves a computer workstation capable of processing video files in a timely manner. This need not be a $10,000+ liquid-cooled digital forensics powerhouse with all the bells and whistles, but a quality processor and video card is a must. A high-quality desktop or laptop computer can serve this purpose. Software may still function on slower machines, and videos will still play, but personnel will spend their time waiting for files to load rather than working on actual cases.

In most agencies, computer purchasing and administration is within the purview of the IT department. While the IT staff can provide recommendations and assistance in purchasing a workstation, it is imperative that video forensic personnel have administrator privileges on the machine. Many

times—and with good cause—IT administrators restrict access to program files and installation ability on networked computers for protection of the entire network. By the nature of video forensics, the installation of various software will be necessary, often from a variety of websites. Personnel must have the ability to perform these tasks without constant reliance on the IT department.

To maintain network security and allow for productivity within video forensic units, many agencies opt to keep video forensic computers off the department's network and dedicate separate Internet access to the forensic workstation. This is often achieved through a separate business Internet line or a dedicated cellular mobile Wi-Fi hotspot. Separating network and Internet access in this manner may carry a slightly increased cost to the agency, but it is regarded as prudent.

Computer Software

Several commercial software packages are available to assist in the acquisition, processing, enhancement, and analysis of digital video files. Goals and functions of the forensic video unit can dictate which software package best suits an agency's needs. Regardless of the function, the nature of forensic science requires that any software be tested prior to use on evidence to ensure that it functions properly and as intended.

Most vendors will permit a free trial period for potential customers to evaluate their product, and agencies should assess all options to see what best fits their specific needs. Despite differences in appearance and some nuances, the underlying science and mathematical calculations in these packages are remarkably similar. For that reason, evaluating software to see what best suits an agency's needs is all the more important. Regardless of the vendor chosen, proper training is integral to using the software effectively, and training should be considered in all budget decisions and cost analysis.

It is worth noting that nearly all forensic video functions can be completed using free open-source software. This software may be just as sound as its commercial counterparts, but it often requires much more manual input and skill from the operator to perform functions. Many free software options are discussed in forensic video training courses, and it is not uncommon to find a combination of both free and paid software in a forensic video expert's toolbox.

Policies and Procedures

The cornerstone of any forensic video unit is the reference material that it is built upon. It is imperative to establish a set of standard operating procedures (SOPs) prior to undertaking any casework. These SOPs can serve not only as a workflow for daily operations, but as an established standard when explaining actions in court. For that reason, any SOP introduced must be built upon a solid foundation.

A number of organizations publish standards and best practices for use in forensic video analysis. These standards and best practices are developed by subject matter experts and often are subject to public comment by the forensic community. Readily available online, the documents can be used as a framework for SOPs and should be referenced within the SOP to bolster validity.

The **Scientific Working Group on Digital Evidence (SWGDE)** develops best practice documents for many areas within digital forensics, including forensic video. These documents are developed with the practitioner in mind and can be used to develop SOPs for many forensic video functions. Core competencies and training requirements are also addressed by the group.[2]

The **Organization of Scientific Area Committees (OSAC) for Forensic Science**, administered by the National Institute of Standards and Technology (NIST), is tasked with developing standards for use throughout all of forensic science, including digital and multimedia evidence. A work in progress, the OSAC registry will serve as a one-stop shop for all standards relating to forensic video once it is fully populated. This will be the yardstick to which all work is compared and can be used to clearly define practices that should be incorporated into an SOP.[3]

The current standards development organization for video forensics is **ASTM International**. While ASTM addresses standards for many industries, a number of them apply to video forensics. These standards clearly define minimum requirements for completing many video forensic tasks and can be easily adapted to SOPs. Additionally, the ASTM standards are the same standards recognized by the OSAC.[4]

There is also a push across all the disciplines in forensic science to achieve laboratory accreditation. This is important to recognize at the onset of any video forensics unit; not only as a possible eventual goal, but as to the possible effects on other elements within a police agency. As a forensic science unit, many forensic video units find themselves housed in the crime lab or digital evidence laboratory chain of command. Should the other disciplines within an agency be accredited, the existing infrastructure will ease the process if or when video forensics is added. It is also important to recognize that some federal grant funding for crime laboratories is dependent on laboratory accreditation or work toward accreditation. If a new video unit is incorporated into an existing accredited lab, it may be necessary for the new unit to also be accredited in order to continue receiving grant funding.

It might seem at first thought that starting a forensic video unit is simple, but doing it right is no small undertaking.

Is a Forensic Video Unit Worth It?

It might seem at first thought that starting a forensic video unit is simple, but doing it right is no small undertaking. While it is easy to recognize the proliferation of video evidence in modern criminal investigations, it is an entirely different undertaking to devote money, time, manpower, and resources to unlock the full potential of video evidence. Agencies, particularly smaller ones, may see this as a barrier to forming a dedicated unit. Initial considerations aside, agencies might also wonder if there will be enough casework to support a full-time staff working solely on video forensics.

Many agencies begin or operate with a video forensics unit that has other assigned duties. Often, these complementary tasks include mobile device forensics, computer forensics, or forensic photography. While those other fields may have some similar knowledge bases in computer science or digital imagery, it is important to recognize that they are all perishable skills. Personnel should be given adequate time to maintain proficiency in the discipline; it should not be expected for staff to rotate a skill set every three to six months and maintain any real competency in video forensics. This will ensure that cases are not only handled more efficiently, but that the work products are also accurate and will withstand any challenges in court. ❖

Notes:

[1]International Association for Identification, *IAI Resolution 2002-12*.

[2]The Scientific Working Group on Digital Evidence (website), www.swgde.org.

[3]National Institute of Standards and Technology, "The Organization of Scientific Area Committees for Forensic Science," April 11, 2016, updated April 11, 2018www.nist.gov/topics/forensic-science/organization-scientific-area-committees-osac.

[4]ASTM International, "Committee E30 on Forensic Sciences," www.astm.org/committee/E30.htm.

PRODUCT FEATURE:

GETTING THE DETAILS RIGHT IS KEY FOR SAFETY GEAR

By Scott Harris, Freelance Writer

For law enforcement, safety gear can take many forms. Some equipment—such as body armor—is of obvious and paramount importance. But many other kinds of gear play a role in officer safety, even though these tools may carry a lower profile than those directly associated with saving lives in the line of fire.

The right communications equipment, for example, can be a matter of life and death for officers, as can the day-to-day equipment that is sometimes unintentionally viewed as an afterthought by some departments—potentially increasing risks for officers.

"Law enforcement has always been a dangerous job, but maybe they do not always have all the tools to do the job safely," said Seth Leyman, president of Communications-Applied Technology (C-AT), a Reston, Virginia, audio communications firm.[1]

Keeping Officers Informed and Connected

Reliable radio systems are indispensable in high-pressure situations. C-AT produces the ICRI Radio Interoperability Gateway System not only to connect different municipal, state, and federal radios, but also to connect telephones, VoIP devices, and other communication devices. The system's capabilities include connections in scenarios over long distances or in areas with traditionally poor reception.

"It provides a connection between multiple agencies," said Leyman. "It could be a benign scenario, or it could be a disaster scenario like an active shooter. The environment for radios is not always perfect. Our equipment is used extensively as a repeater to connect your own agency with itself, but you could be [at a distance]."

The ICRI requires minimal power, making it unnecessary for users to find an electrical outlet to power up the device. "You can use AA batteries instead of worrying about where or how to charge it," Leyman said.

A reliable system that connects different radios from different agencies improves not only the safety of all first responders by enabling deconfliction, allowing collaboration, and sharing key information (such as whether a suspect who has evaded police capture is armed), but also the safety of civilians those responders are attempting to reach by improving police response or facilitating access to an active crime scene.

Lightweight, easy-to-carry banners can be used to identify officers not in uniform to increase safety on-scene.
Photo courtesy of DSM Safety Products.

"In many cases, the agencies are told that if you can't communicate with each other, then you have to back out of a situation, because without that communication you can be in jeopardy very quickly," Leyman said. "If there's an active shooter scenario, you have to communicate outside, then you have to go inside and monitor communications both inside and outside the building."

Effective communication happens in any number of ways. In certain situations, an officer's uniform can become a powerful platform for communication.

To illustrate, DSM Safety Products, based in Sparks, Nevada, offers the "Don't Shoot Me" banner.[2] Designed by a former SWAT sergeant, the lightweight banner identifies non-uniformed officers as police, to avoid mistaken engagement by uniformed officers during an active shooter or similar incident. The goal of the banner is to prevent tragedies that can occur when non-uniformed officers are mistaken as suspects or perpetrators. There are also similar banners for medical and security staff, among other personnel who might be on scene.

Custom Helmets to Increase Officer Safety

Many police departments regard some safety gear, such as helmets, with an almost literal one-size-fits-all sense. At Super Seer Corporation, based in Evergreen, Colorado, expertly trained craftsmen custom-make 12 different helmet models for police use, designed for situations ranging from motorcycle units to mounted officers.

"We are a helmet manufacturer," said Super Seer Vice President Kevin Smith. "We make each helmet to order. Our minimum order number is 1, not 1,000. These are made by hand…. They are personalized, and you can customize them practically endlessly."[3]

The first helmet safety issue that Super Seer addresses is fit. While other helmet manufacturers use padding, Super Seer uses hard shells to ensure each helmet fits more snugly and over the long term.

"The one-size-fits-all mentality is something police departments accept, but it's not a good mentality," Smith said. "A helmet can rotate around on you if it's not properly fitted."

The second safety issue is that different situations have different helmet needs. In other words, purchasing a helmet with a certain rating is not necessarily optimal for different scenarios, even if that rating is high.

"If your main threat is rocks, bricks, or bottles, you'd want a riot helmet," Smith explained. "A ballistic helmet can obviously

AMERICAN MADE
POLICE HELMETS

Since 1967, Super Seer has been manufacturing law enforcement helmets designed specifically for police officers. Every **SEER HELMET** is made by hand at our helmet factory in Colorado, and every material used in making a Seer Helmet has been carefully selected to stand up to the rigors of law enforcement duties. Our complete line of riot, motorcycle, corrections, mounted, general duty and ballistic helmets are as unique as the officers who serve these special units. For information or to request a price quote, please visit our website.

SUPER Seer®

superseer.com
800-645-1285

Riot Helmets

Mounted Helmets

Motorcycle Helmets

Corrections Helmets

Ballistic Helmets

Law enforcment–specific disposable gloves are more durable, better protecting the officer.

Photo courtesy of Summit Glove.

stop gunfire, but it is not as good at defending against rocks, bricks, or bottles. If you fall from a horse, that's different from falling from a motorcycle. We take a look at your specific threats and threat levels and assign a helmet accordingly."

Super Seer offers different models for motorcycles, mounted, riot and tactical, and corrections environments.

Fitting Like a Glove

In some cases, gloves are an afterthought. However, inferior gloves can leave officers vulnerable to bloodborne diseases, dangerous drugs, and other substances.

"Lots of police departments just go to big-box stores to buy gloves," said James Hull, president of Summit Glove in Minerva, Ohio. "But our glove is strong enough for law enforcement."[4]

Standard disposable gloves can develop tiny holes that can undermine their protective capabilities. But Summit's gloves are examination grade and approved by the U.S. Food and Drug Administration. The gloves feature extra thickness in the palm and fingertips and wick away moisture to help officers maintain their grip even in wet conditions. The gloves are also heat and cut resistant.

"We've taken high-quality formulas and made them applicable to law enforcement," Hull said. "A lot of times, gloves would tear, and people didn't even understand that there was a problem with quality."

Hull, who recently began selling gloves to the Boston, Massachusetts, Police Department, pointed to crime scenes or vehicle collisions as areas where strong gloves are needed to protect officers from injury or disease. The ongoing crisis around opioids like fentanyl—which can be absorbed through the skin—also increases the need for higher-quality gloves.

Hull acknowledged that Summit gloves are more expensive than standard disposable gloves, but he made the case that the high-quality gloves are worthy investments. "There really hasn't been a standard, high-quality product that law enforcement officers have been able to utilize," Hull said. "It's not low cost, but it is high quality."

For more extreme situations, the Safariland Group, headquartered in Ontario, California, designed the Defender II glove. A double layer of goat skin and steel-reinforced knuckles provide durability and abrasion resistance. The Defender II also has design elements that allow for maximum dexterity.[5]

Safariland offers several different gloves, but one of the more novel models created with safety in mind is the Task High Viz glove. Available in bright orange or yellow, the gloves were developed for increased safety and effectiveness in traffic management and similar duties, particularly in lower-light conditions.

Breathe Easy

Gas masks and respirators might not be used every day, but when the time comes for officers to don them, it is critical that they work properly. Sirchie, based in Youngsville, North Carolina, is well known as a leader in crime scene and forensic solutions. Among other equipment for law enforcement, the company offers a range of gas masks, respirators, and filters.[6]

One such respirator, the Avon C50 Air Purifying Respirator is certified for use in chemical, biological, radiological, and nuclear defense (CBRN) situations. The purifier offers high protection, a good field of vision, and superior comfort, according to company information.

Another model, the Avon PC50 Air Purifying Respirator is not certified for use in CBRN scenarios, but provides protection against contaminated particles, gases, and vapors. It's mainly designed for corrections, riot control, border patrol, and similar situations. Different CBRN filters are available for both models.

Safety gear is a priority for all agencies, but as discussed herein, it's important to look beyond the obvious protective gear to the details, such as communication tools and tactical accessories, to ensure officers are protected to the fullest in any situation they might encounter. ❖

Notes:

[1]Seth Leyman (president, Communications-Applied Technology), telephone interview, April 15, 2018.

[2]DSM Safety Products, http://www.dsmsafety.com.

[3]Kevin Smith (vice president, Super Seer Corporation), telephone interview, April 10, 2018.

[4]James Hull (president, Summit Glove), telephone interview, April 16, 2018.

[5]The Safariland Group, http://www.safariland.com.

[6]Sirchie, http://www.sirchie.com.

PRODUCT FEATURE:

SAFETY GEAR PROVIDERS

For contact information, please visit www.policechiefmagazine.org.

Aker Leather Products

ATS Armor

Battle Rifle Company

BPS Tactical

Communications-Applied Technology

Edge Tactical Eyewear

Eiseman-Ludmar Co, Inc.

EK USA Inc.

Fox Tactical

Galls

GH Armor Systems

Lund Industries, Inc.

Markl Supply Company

Police Bike Store

Pro Wear Gear

Safevision LLC

Sirchie

Super Seer Corporation

T3 Motion Inc.

The Safariland Group

The York Company

TigerLight Inc.

Twitco Distributing

Better value, better gear.

Newly designed

- More adjustability
- Superior protection
- Greater maneuverability
- Maximized comfort
- Enhanced convenience

TAC Commander™

Prepare today for tomorrow.

SIRCHIE®
Command Every Scene®

Leading competitor

TacCommander™

(800) 356-7311 sales@sirchie.com www.sirchie.com

The FBI's NIBRS Transition: Questions and Answers

By Jeffrey Fisher, Writer-Editor, Crime Data Modernization Team, FBI

On January 1, 2021, the Federal Bureau of Investigation (FBI) will retire the Summary Reporting System (SRS), the Uniform Crime Reporting (UCR) Program's longtime crime data collection system. Thereafter, the FBI's UCR Program will collect crime statistics only through the National Incident-Based Reporting System (NIBRS), making it the only nationwide format for crime statistics in the United States. To prepare for this, the FBI is working with the U.S. law enforcement community to ensure agencies are ready to participate before the final changeover date. During the discourse around this shift, common questions arise from law enforcement executives seeking to better understand why the FBI is moving to NIBRS and how the change will affect their agencies.

Q: How is NIBRS better than SRS? What does "incident-based" mean?

A: To understand the advantage of NIBRS' incident-based data over SRS, think about the way a sports fan understands a baseball game. Summary data, such as that collected in SRS, is like the scoreboard in that it counts a few pieces of basic information such as runs scored and current number of outs. However, the scoreboard does not track detailed information. A scoreboard can report one team scored eight runs while the other team scored five runs, but it does not offer the details illustrating how the game actually went. Which players scored the most runs? How many steals were unsuccessful? When did pitchers throw curveballs? A small amount of information on a scoreboard is not very useful for really understanding what happened, but a full play-by-play commentary is. If SRS is the scoreboard, NIBRS is the full-color commentary.

SRS, like a baseball scoreboard, captures only basic information.

NIBRS is a wide-ranging system for collecting crime data from across the United States. The NIBRS data set provides detailed statistics about crime to help law enforcement agencies, communities, residents, researchers, and public leaders make informed decisions about how to understand and combat crime. Incident-based data help to provide a fuller understanding of the components of crime. NIBRS provides specifics about crime, including the following incident elements, as applicable to each crime:

- Arrestee age, race, and sex
- Bias motivation
- Circumstance
- Drug quantity
- Location type
- Method of entering premises
- Offender age, race, and sex
- Offender drug and computer use
- Offense attempts and completions
- Property stolen or damaged
- Relationship between victim and offender
- Time of day
- Type of weapon or force
- Victim age, race, and sex[1]

Simply put, NIBRS is better at collecting attributes of crime data. Unlike the SRS tally of crimes with minimal details, NIBRS captures many data elements and values to provide a more comprehensive picture of an entire criminal incident. This is what is meant by the term "incident-based." NIBRS also captures data on many types of offenses not included in SRS, such as extortion and bribery.

SRS served the United States well for decades, but NIBRS is a superior system that provides the more complex information needed for modern policing and planning. Using the superior data set provided by NIBRS, agencies can consider how to better allocate and utilize resources.

Q: How will the FBI's UCR Program move forward after the transition?

A: In 2021, the FBI will retire *only* the SRS. Although the time of SRS will have passed, the FBI's UCR Program will maintain a historical archive of SRS data, as well as comparative future data derived from NIBRS that students and analysts may access and study.

Also, the FBI plans to continue publishing SRS data even after the NIBRS transition of January 1, 2021. The FBI will do this by converting the NIBRS data into SRS data, as the FBI has been doing in its annual *Crime in the United States* publication. The purpose of this is to provide agencies with the ability to make "apples-to-apples" comparisons and conduct trend analyses across the years of the NIBRS transition.

Other UCR data programs and collections will continue, including the following resources:

- *Law Enforcement Officers Killed and Assaulted*
- Hate Crime Statistics
- Cargo Theft
- Human Trafficking
- Other miscellaneous studies and publications

Q: Will the transition to NIBRS affect an agency's crime rate, and how can that be explained?

A: NIBRS provides a more complete count of crimes than SRS. Law enforcement agencies can explain the differences between the SRS and NIBRS figures to the news media and the general public by stating NIBRS simply does a better job of counting crimes that SRS had previously

been omitting. Agencies can remind the media and the public that complete, transparent accounting of data is crucial for truly understanding crime and strategizing solutions for a community's crime problems.

Compared with SRS, NIBRS captures a more transparent and complete measurement of crime. NIBRS does this in several ways. For instance, SRS uses a "hierarchy rule," in which only the most severe crime within an incident was counted, whereas NIBRS will count up to 10 offenses per incident. In addition, NIBRS has the capability to collect data about crimes that were not counted by SRS.

Some agency officials may be concerned about the difference between SRS and NIBRS figures and how the media or general public might perceive a seeming uptick in crime. To address this concern, the FBI conducted a study, *Effects of NIBRS on Crime Statistics*. The study found the difference between SRS and NIBRS figures is fairly small on average, although local and regional trends may vary. The FBI quantified the difference between SRS and NIBRS figures from a nationally representative sample of 2014 data by converting NIBRS data into equivalent SRS data. The difference was negligible for the offense of homicide because it is the top of the SRS hierarchy of offenses. For other SRS offenses, the FBI found minimal differences with NIBRS data. The offenses were impacted as follows:

- Rape: No effect
- Robbery: Increased 0.6 percent
- Aggravated Assault: Increased 0.6 percent
- Burglary: Increased 1.0 percent
- Larceny: Increased 2.6 percent
- Motor Vehicle Theft: Increased 2.7 percent
- Total SRS Offenses: Increased 2.1 percent

Some agency officials may be concerned about NIBRS counting up to 10 offenses per criminal incident, thinking that the reporting requirements for those additional offenses might bring a significant increase in the reporting workload under NIBRS. However, the FBI study found that only 10.6 percent of criminal incidents involved multiple offenses.[2] The FBI's study is available to the public, so agencies can also cite it as a resource and refer interested parties to it.

Q: Must every agency participate in NIBRS?

A: Because of the FBI's total commitment to NIBRS, after the January 1, 2021, deadline, if agencies do not participate in NIBRS, their data will not be included in the FBI's U.S. crime statistics collection. The Uniform Federal Crime Reporting Act of 1988 mandates federal participation in UCR, but the FBI does not have legal authority to make NIBRS participation mandatory for nonfederal agencies.[3] The FBI makes UCR programs such as NIBRS available to the U.S. law enforcement community, but nonfederal agency participation is voluntary.

Agencies should also be aware of how the NIBRS transition could affect their funding. Many agencies receive grant funding based on their SRS participation. If these agencies do not transition to participating in NIBRS, those agencies could lose their SRS-based grants, such as Edward Byrne Justice Assistance Grant (JAG) funding.

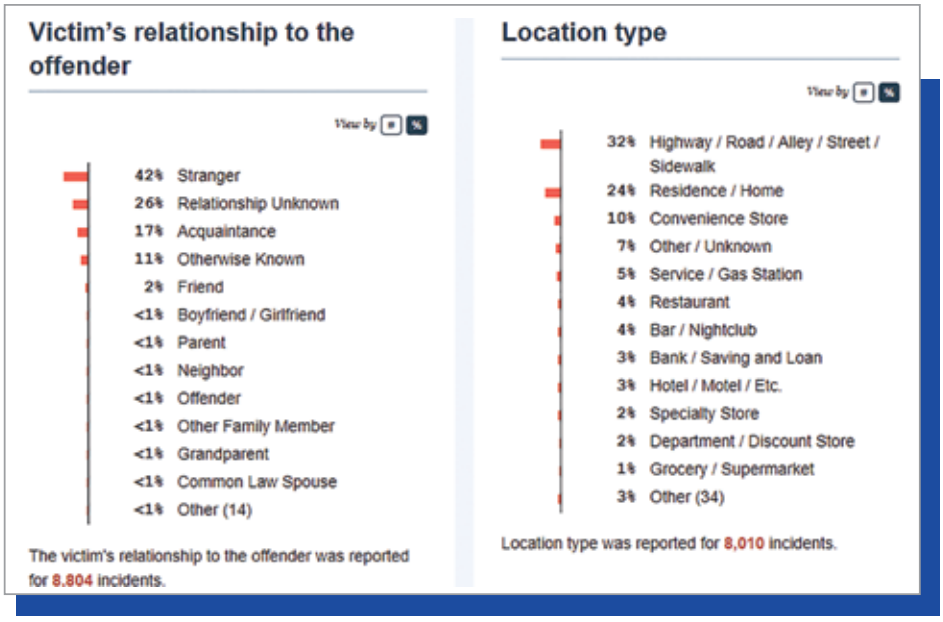
To help with an agency's transition, the FBI's UCR Program maintains a NIBRS certification program to ensure participating agencies are able to adhere to NIBRS data standards. However, agencies may expand their own data collection requirements and still participate in NIBRS, provided that their NIBRS submissions meet the FBI's technical specifications. For example, agencies can collect more comprehensive and detailed crime data about drugs than NIBRS specifies, if they wish. The agencies can analyze the extra data at the local level, and the agencies can still participate in NIBRS if the additional data elements are removed from their NIBRS submissions before they are sent to the FBI.

Q: Does agency size, type, or location impact the utility of NIBRS?

A: Some larger agencies may be reluctant to participate in NIBRS because of the large number of incidents they have to report. Some smaller agencies may think they cannot participate in NIBRS because of their small budgets and resources. Some agencies, such as task forces or park police, may think NIBRS is not built to reflect their type of agency or mission. However, NIBRS is intended for all sizes and types of agencies in all regions of the United States.

Consider these examples of the variety of agencies participating in NIBRS during the 2016 reporting year, encompassing many sizes, locations, and geographical factors:

- The Memphis Police Department in Tennessee has 1,978 officers representing a population of 656,434 residents, making it one of the largest agencies participating in NIBRS for 2016.[4]
- The Booneville Police Department in Kentucky has 1 officer representing a population of 75 residents, making it one of the smallest agencies currently participating in NIBRS.[5]
- The Sumas Police Department in Washington is headquartered about 400 yards from the Canadian–U.S. border.
- The Indian Lake Police Department in Texas is located about nine miles from the Mexican–U.S. border.
- The Leadville Police Department in Colorado is one of the highest-altitude NIBRS agencies at about 10,200 feet above sea level. Its officers deal with nine months of snow per year while protecting residents and visitors.[6]
- The Mackinac Island Police Department in Michigan is located on a three-mile-long island in Lake Huron. Its officers serve a community that is connected to the mainland by ferries and an airport.



NIBRS includes much more information, as in this capture of a state's robbery data about victim-offender relationship and location type from the FBI's Crime Data Explorer. SRS does not collect this information at all.

Q&A

NIBRS' breadth and level of detail can provide valuable insight to agencies in serving and protecting their communities.

Agencies across the United States have different geographic challenges and considerations, and NIBRS is designed to capture valid crime data to serve all areas. For example, NIBRS can capture data to distinguish types of stolen property that might be more typically found in some areas than in others, such as livestock, office equipment, or—as in the case of Mackinac Island—watercraft. NIBRS also distinguishes various drug types involved in crimes, making it useful for tracking drug trends in different areas.[7] In order to help agencies better track data about where crimes occur, NIBRS captures data about such varied location types as amusement parks, wharfs, farms, military installations, tribal lands, and even cyberspace.[8]

NIBRS is also designed for all types of U.S. law enforcement agencies. During the 2016 reporting year, in addition to the "typical" city, county, and state police agencies, NIBRS participants included a wide range of other agencies, including the following agencies:

- Delaware Division of Fish and Wildlife
- South Carolina Ports Authority
- Rhode Island Department of Environmental Management
- Kentucky Fairgrounds Security
- Colorado Mental Health Institute
- Kanawha County Parks and Recreation in West Virginia
- New Hampshire Liquor Commission
- South Carolina State Museum
- Tonkawa Tribal Police Department in Oklahoma
- Montana State University[9]

Thanks to such diversity in participating agencies, NIBRS provides a more detailed look at crime statistics in specific areas and demographics that might otherwise be overlooked. This breadth and level of detail can provide valuable insight to agencies in serving and protecting their communities.

The FBI realizes an agency's size, type, or location brings different challenges regarding such factors as budgets, crime trends, populations represented, or environmental conditions encountered. These differences are why the FBI encourages agencies to seek advice from the FBI's NIBRS help staff. The FBI also encourages agencies to help each other with solutions such as pooling budgets, sharing technical resources, or arranging for larger agencies to "cover" the reporting of smaller agencies.

Q: Where can agencies find more information about NIBRS?

A: Agencies wishing to learn more about the NIBRS transition can find several other articles the FBI has authored in recent months.

- "NIBRS: The Future of U.S. Crime Data," detailing the FBI's long-term plans for NIBRS development.[10]
- "The Texas Transition to NIBRS," showing how the Texas Department of Public Safety has been working toward statewide NIBRS participation.[11]
- "SRS to NIBRS: The Path to Better UCR Data," explaining the history and reasons for the FBI's decision to retire SRS and collect data only through NIBRS.[12]
- "Going NIBRS, Part 1: Two States Share Their Stories," discussing how the Minnesota Bureau of Criminal Apprehension has been preparing for the NIBRS transition.[13]
- "Going NIBRS, Part 2: Two States Share Their Stories," detailing the Georgia Bureau of Investigation's proactive approach to enhancing crime data.[14]

The FBI publishes general information about NIBRS on its website (https://ucr.fbi.gov/nibrs-overview). Also, the UCR Program has recently unveiled its Crime Data Explorer to make NIBRS crime data and analytical tools available to the public at https://crime-data-explorer.fr.cloud.gov. NIBRS support staff can be reached by email at ucr-nibrs@fbi.gov or by phone at 304-625-9999. ❖

Access this article online for links to the resources listed in this article.

Jeffrey Fisher is a writer-editor with the FBI's Crime Data Modernization Team. He has an MS from West Virginia University, and he has worked for the FBI for 21 years as a forensics expert, manager, and writer. He can be reached by email at jfisher2@fbi.gov.

Notes:

[1]FBI, "Incidents and Offenses," *NIBRS 2016* (2017), https://ucr.fbi.gov/nibrs/2016/resource-pages/incidents-and-offenses-2016_final.pdf.

[2]FBI, "Effects of NIBRS on Crime Statistics," *NIBRS 2014* (2015), https://ucr.fbi.gov/nibrs/2014/resource-pages/effects_of_nibrs_on_crime_statistics_final.pdf.

[3]28 U.S.C. §534(a) and (c).

[4]FBI, *Crime in the United States 2016*, table 26: Tennessee, https://ucr.fbi.gov/crime-in-the-u.s/2016/crime-in-the-u.s.-2016/tables/table-26/table-26-state-cuts/table-26-tennessee.xls.

[5]FBI, *Crime in the United States 2016*, table 26: Kentucky, https://ucr.fbi.gov/crime-in-the-u.s/2016/crime- in-the-u.s.-2016/tables/table-26/table-26-state-cuts/table-26-kentucky.xls.

[6]Leadville, Colorado, "The High Altitude Life," https://leadville.com/the-high-altitude-life.

[7]FBI, *National Incident-Based Reporting System (NIBRS) Technical Specification Version 3.0 January 2017 Technical and Operational Update (TOU)* (Clarksburg, WV: FBI, 2017), 14–15, 19–20, https://ucr.fbi.gov/nibrs-technical-specifications-version-3.0-technical-and-operational-update-january-2017.

[8]FBI, *National Incident-Based Reporting System, 2016*, "Data Tables," Tables with All Offenses, Location, 2017, https://ucr.fbi.gov/nibrs/2016/tables/data-tables.

[9]FBI, "United States, Offense Type by Agency, 2016," https://ucr.fbi.gov/nibrs/2016/tables/state-pdfs/united_states_offense_type_by_agency_2016.pdf/at_download/file.

[10]Jeffrey Fisher, "NIBRS: The Future of U.S. Crime Data," *The Police Chief* (October 2017): 48–55, http://www.policechiefmagazine.org/nibrs-the-future-of-u-s-crime-data.

[11]FBI, "The Texas Transition to NIBRS," *CJIS Link*, December 6, 2017, https://www.fbi.gov/services/cjis/cjis-link/the-texas-transition-to-nibrs.

[12]FBI, "SRS to NIBRS: The Path to Better UCR Data," *CJIS Link*, March 28, 2017, https://www.fbi.gov/services/cjis/cjis-link/srs-to-nibrs-the-path-to-better-ucr-data.

[13]FBI, "Going NIBRS: Two States Share Their Stories: Minnesota's Transition to NIBRS," *CJIS Link*, April 11, 2017, https://www.fbi.gov/services/cjis/cjis-link/going-nibrs-part-1-minnesota-transition.

[14]FBI, "Going NIBRS: Two States Share Their Stories: Georgia's Movement Toward NIBRS," *CJIS Link*, April 27, 2017, https://www.fbi.gov/services/cjis/cjis-link/going-nibrs-part-2-georgia-transition.

LEADERSHIP'S EVOLUTION

Celebrating 125 Years of Progress

Experience and learn about the latest law enforcement technology you can bring back to your agency.

After visiting with exhibitors stop by:

- The Hub to learn about IACP products and services
- Entertainment Zone to see news and sports updates
- Relaxation Zone to rest and recharge
- Connection Zone to check in with free Wi-Fi

IACP 2018 October 6–9 Orlando FLORIDA

REGISTER AND RESERVE YOUR HOTEL TODAY AT
theIACPconference.org

Thank you to Industry Leader Sponsors:

AXON

FIRSTNET Built with AT&T

MOTOROLA SOLUTIONS

verizon

Race to the Cloud...

PROCEED WITH CAUTION

By Scott A. Vantrease, Assistant Special Agent in Charge, U.S. Department of Health and Human Services, Office of Inspector General, Office of Investigations, Digital Investigations Branch; Jim Emerson, Lieutenant Colonel (Ret.), U.S. Marine Corps, Chair, IACP Computer Crime and Digital Evidence Committee; and Eldon Amoroso, OOM, Senior Director (Ret.), London Police Service, Canada

There are speed limits for most roads and waterways, with the caveat known well by all—one should drive only as fast as conditions allow. A great rule of thumb to avoid damage during driving, boating, and even technology adoption is to operate as the circumstances permit. Just as a road might have caution signs regarding weather or unexpected turns, those agencies that "race to the cloud" are cautioned to reduce their speed and review all the conditions that may impact an agency before just taking off like a muscle car on an open freeway. When a law enforcement executive is evaluating historical infrastructure for an IT vendor, the executive remains the driver, and the vendor is the car salesman and mechanic. When evaluating a move to the cloud, not only does the executive allow someone else to drive, but, in many cases, that person also is controlling the vehicle remotely rather than onboard. This approach makes the risk to the cargo—confidential data—entirely different than traditional infrastructure where, if there were issues, an executive could address the matter and exchange, repair, or otherwise solve the problem. Regardless of the situation, the executive remained in control. Given the technical and business realities of the cloud, that model is flipped, especially regarding risk, in that the executive sends his or her agency's precious cargo to be controlled by a third party.

Understanding Cloud Storage and Cloud Services

It is important to know what is meant by "cloud" storage and services. Law enforcement executives should understand that cloud storage and services are not anything new; instead, they are a modernized and updated approach to past technology. Current law enforcement leaders came up through their careers with the original "cloud" (actually a distributed computing model connected by telecom-based transfer of data), meaning they accessed systems through a terminal connected to a "mainframe," which was processing data, and storage was located elsewhere. Today's definition of cloud storage and resources is

> *a computing model in which data is stored on remote servers accessed from the internet, or "cloud." It is maintained, operated and managed by a cloud storage service provider on storage servers that are built on virtualization techniques.*[1]

Cloud services and resources are simply resources and services, such as various programs like email, that cloud vendors provide. What this means to law enforcement executives is that agency data will not be stored in their departments or even within their municipalities, but stored instead by a contracted service while remaining accessible to the agency.

Acquisition and Implementation of Cloud-Based Technology

With any significant decision, the steps for acquiring and implementing cloud resources should follow similar processes to other technology purchases. Most technology decisions made by law enforcement executives are about products and support; however, moving an agency and its data into the cloud contains a significant delegation of responsibility. Complex services in the hands of third parties represent a different level of displaced risk and require a different level of due diligence and vendor management than seen in other acquisitions. Selecting and moving services to a cloud services provider should be viewed more like hiring a vendor to process a crime scene and handle evidence than providing computing services. While a vast majority of vendors are technically qualified, the law enforcement executive involved in such decisions must establish why the vendor should be trusted to handle the data ethically. Additionally, an effort must be made to determine how to reliably measure the vendor's performance in advance, with the question of most importance being "What ensures prioritization of my interests in the field of other clients that contract with this

Advance Registration Form

Register online at *theIACPconference.org*

IACP 2018
October 6–9, 2018
Orange County Convention Center
Orlando, Florida
theIACPconference.org

Use this form to save on registration fees until August 22, 2018. Beginning August 23, 2018 only online registrations will be accepted. Questions? Call 800-THE-IACP.

WAYS TO REGISTER

ONLINE

Go to **theIACPconference.org** and click on **REGISTER NOW.**

Only credit card payments are accepted online. Online registration will be open through the conference.

BY FAX

Fax completed forms with credit card payments or Purchase Orders to: **703-836-4543.**

BY E-MAIL

E-mail completed forms to **conf2018@theiacp.org.** Due to registration volume, we cannot confirm fax receipt.

BY MAIL WITH A CHECK

Mail completed forms with checks to:
IACP Conference Registration
PO Box 62564
Baltimore, MD 21264-2564 USA

BY MAIL WITH A PURCHASE ORDER

Mail completed forms with Purchase Orders to:
IACP Conference Registration
44 Canal Center Plaza, Suite 200
Alexandria, VA 22314 USA

IN PERSON

Walk-in registration opens October 5, 2018, at 1:00 p.m. at the Orange County Convention Center – West Building, 9800 International Drive, Orlando, FL 32819

☐ **YES! I would like to receive emails from IACP exhibitors regarding their conference activities and products.**

* Full conference registration fee includes access to all general sessions, workshops, receptions, Expo Hall, and Chiefs Night.

† Family refers to a spouse or family member, not a business associate or fellow law enforcement colleague. ONLY the family member's name, city, and state will appear on their badge. Family members do not receive certificates for workshops.

Do NOT mail and fax form — charges may be duplicated. A cancellation fee is in effect through October 3, 2018. No refunds on or after October 4, 2018. Registration and attendance at IACP events constitutes an agreement by the registrant to the IACP's use and distribution (both now and in the future) of the registrant or attendee's image or voice in photos, images, video and/or audio recordings of such events without compensation or approval rights. All photos, images, and recordings are the property of IACP.

Source Code: PCM

CHECK ONE:

☐ I am an IACP Member; Membership Number _____
☐ I am a Non-Member
☐ I am applying now for Membership (Use Box "B" below to Join)
☐ I am the spouse or family member of _____ Their Member# _____

Full Name _____

First Name for Badge _____

Title/Rank _____

Agency/Organization _____

Agency Address _____

City _____ State _____

ZIP/Postal Code _____ Country _____

Phone # _____ Fax # _____

Email Address _____

FAMILY — complete a duplicate registration form if using different payment method.†

Name _____

Children (5 and Under) Name(s) and Age(s) _____

Children (6–18) Name(s) and Age(s) _____

A. CHECK APPROPRIATE REGISTRATION TYPE

☐ IACP Member* $425
☐ First Time IACP Member* $370
☐ Non-member* $600
☐ Family Member*† $150
☐ Children 6–18* $45
☐ Children 5 and under* . . . . . FREE
☐ Expo Pass for Public Safety Personnel . . . . . FREE

1-Day Pass and 2-Day Pass Registration will open online August 23, 2018.

B. IACP DUES

☐ YES! I would like to join the IACP and take advantage of the First Time Member Registration Rate of $370 (see the website for membership benefits and criteria), **plus the dues amount below:**

☐ Active Member $150
☐ Associate Member – General $150
☐ Associate Member – Leader of Tomorrow Sworn Officer $75
☐ Associate Member – Academic $150
☐ Associate Member – Service Provider $250

C. ANNUAL BANQUET TICKETS *(Optional)*

☐ YES! I would like to purchase tickets for the **Annual Banquet** to be held on Tuesday, October 9, 2018.

Tickets $100 each; # of tickets: _____

No refunds. Pre-Conference ticket sales end October 3, 2018 and will continue onsite October 6–9, 2018.

PAYMENT (No Registrations will be processed unless accompanied by payment in full.)

TOTAL AMOUNT TO BE CHARGED (Add A, B and C): $ _____

☐ **Purchase Order.** PO# _____

☐ **Check.** Make checks **payable to IACP** (U.S. dollars, drawn on U.S. banks only) and mail full payment (no cash) with completed form to: IACP Conference Registration, P.O. Box 62564, Baltimore, MD USA 21264-2564

Please charge my credit card: ☐ Visa ☐ MasterCard ☐ American Express ☐ Discover

Acct. # _____ Exp. Date _____

Cardholder's Name _____

Billing Address _____

Signature _____

Orlando Hotel Information

IACP 2018
October 6–9, 2018
Orange County Convention Center
Orlando, Florida
theIACPconference.org

Book early for best rates and selection at theiacpconference.org.

Questions? Contact onPeak, the official IACP 2018 housing partner, at **iacphotels@onpeak.com** or 1.866.524.7456.

Official IACP 2018 Hotels	Rate
1 Avanti Resort	$99*
2 Castle Hotel	$199
3 Courtyard International Drive	$179
4 Crowne Plaza Orlando Universal	$172
5 Days Inn Convention Center	$105*
6 DoubleTree Resort Orlando – International Drive	$119*
7 Embassy Suites by Hilton International Drive Convention Center	$235
8 Embassy Suites by Hilton Orlando International Drive/I-Drive 360	$204
9 Extended Stay America Convention Center – Universal Blvd	$95*
10 Fairfield Inn & Suites at SeaWorld	$154
11 Fairfield Inn & Suites Orlando International Drive Convention Center	$154
12 Hampton Inn by Hilton Orlando Convention Center	$139
13 Hilton Garden Inn Orlando at SeaWorld	$149
14 Hilton Grand Vacations at SeaWorld	$129
15 Hilton Orlando	$269
16 Homewood Suites by Hilton Orlando Convention Center	$179
17 Hyatt Place Orlando – Convention Center	$159
18 Hyatt Regency Orlando	$269
19 Renaissance Orlando at SeaWorld	$219
20 Residence Inn Orlando Convention Center	$176
21 Residence Inn at SeaWorld	$169
22 Rosen Centre	$249
23 Rosen Inn at Pointe Orlando	$92*
24 Rosen Plaza	$229
25 Sonesta ES Suites Orlando	$199
26 Springhill Suites Orlando Convention Center	$171
27 Springhill Suites at SeaWorld	$159
28 Westgate Lakes Resort	$92*
29 Westgate Palace Resort	$177
30 Wyndham Orlando Resort International Drive	$147

*Per Diem Rate Available

Rates as of 10/6/17. Rates are subject to change.

IACP CLOUD RESOURCES

Access this article online (www.policechiefmagaazine.org) to find links to these resources or search "cloud" on the IACP website.

- *Guiding Principles on Cloud Computing in Law Enforcement*
- *Cyber Report Card*
- "Sharing and Safeguarding Information" (IACP blog post)
- "Challenges with Big (Data) Storage During Forensic Investigations" (IACP Cyber Center blog post)
- "Embracing the Cloud: How Third-Party Digital Evidence Can Make the Case" (*Police Chief* article)
- "In the Cloud: An Easy Path to Efficiency" (*Police Chief* product feature)
- "More Efficiency, More Effectiveness Lie in the Cloud" (*Police Chief* product feature)
- IACP Law Enforcement Cyber Center

vendor?" Law enforcement executives will find that rather than reducing oversight, they will increase their participation in vendor management. When selecting a cloud services vendor, the executive's due diligence is vital—and the level of research and oversight needed for such a transition may be new to the average executive and to agency staff.

The law enforcement executive should carefully weigh all factors, some of which will be elaborated on here, and make prudent decisions. In some instances, the law enforcement executive will have a significant say; in others, the executive's input will almost appear an afterthought by information technology (IT) staff. In either situation, the law enforcement executive must be able to identify challenges and discuss them with an eye on protecting department data and the department's image. If an agency does not have an established risk management framework going into the process, it is facing a potential increase in risk and will not be prepared to properly articulate existing risk concerns.

It is easy to overlook simple resources when confronted by such an enormous undertaking for which the law enforcement executive may have little background or knowledge. Regardless of the size of the agency, some essential guidelines are available from the IACP, including *Best Practices Guide: Acquisition of New Technology*.[2] This short guide, designed for smaller police departments, provides critical steps in understanding the acquisition and implementation of technology. The stages outlined in this guide are crucial to acquiring cloud-based technology.

Throughout the evaluation of cloud services and vendors, law enforcement executives should utilize the practices outlined in the aforementioned guide, in conjunction with the following universal principles provided in the 2014 *IACP Technology Policy Framework*:

- Specification of Use
- Policies and Procedures
- Privacy and Data Quality
- Data Minimization and Limitation
- Performance Evaluation
- Transparency and Notice
- Security
- Data Retention, Access, and Use
- Auditing and Accountability[3]

Data and Information Security

Some vendors will say that cloud infrastructure is more secure than traditional localized storage. While this is probably true in theory, law enforcement executives need to consider both internal and external security concerns before making the decision to store data in the cloud. Internally, the law enforcement executive must consider what data the agency wishes to store in the cloud. Is it report documents, photos, video evidence, or other data? The information that law enforcement receives is vital to the safety and well-being of officers, professional staff, and the people law enforcement serves and protects. For operational data (CAD, reports, etc.), law enforcement executives must talk to their IT security partners and the potential providers to ensure appropriate encryption and access security exists. For photos and video, who will have access to view, copy, or edit the files? A failure to secure data at this level can cause irreparable harm to lives and property, as well as an agency's reputation.

Externally, law enforcement executives have a responsibility to evaluate the security of the provider. The executive must be able to assess a vendor's security, as well as assess vendor risk—technical issues, human error impacts, business requirements, operational requirements, and so forth. Just because a municipality's IT staff has identified an acceptable downtime for cloud services is, for example, 36 hours, based upon the needs of the parks department, such downtime may be disastrous for the law enforcement executive and the agency. For this reason, it will be important for the executive to identify what direct security and information security management the agency or municipality has.

There should also be an evaluation of the vendor's transparency for the law enforcement environment. This should include a clear understanding of whether there is segmentation (ability to keep sensitive data separate from other data for security); rapid adjustment of systems (backup plan if something happens to a data center); and even incident response (clear incident response plan and the notification process and timeline for data compromises or breaches). Information security is about confidentiality, access, and integrity of data and those systems supporting the data. From the perspective of cloud storage, virtualization, distribution, comingling, and other related technology features, it is critical for a law enforcement executive to understand how to approach the agency's portion of the risk—and that the interaction with cloud vendors might be much more complicated than interactions with other vendors and service providers.

A law enforcement executive has to consider not only what happens when an incident occurs, but also how much information he or she will receive and how quickly. In the day and age of transparency, if information is not readily available, it may appear that the agency is concealing the incident, raising trust issues both internally and with the citizens the agency has vowed to protect. It is for these reasons that the law enforcement executive must review all language that might impact or involve the agency in any potential contract. The security a vendor will provide will match only what is in the contract, so this should be reviewed with careful consideration to ensure compliance with an agency's policies, procedures, and plans, such as a current incident response plan. The vendor's compliance with an agency's related requirements strengthens the agency's ability to update policies, procedures, incident response plans, and related elements to comply with updated legal decisions or other needs without requiring a new contract. The evaluation should also include measuring contract language against relevant standards, such as those available from the Cloud Security Alliance (www.cloudsecurityalliance.org); U.S. Department of Commerce, National Institute of Standards and Technology (www.nist.gov); or other standards provided by a jurisdiction's government.

3 Steps to Successful Acquisition of New Technology

1. The acquisition plan
2. Acquisition and delivery
3. Implementation and training

Cloud Storage: Capacity, Costs, and Location

Another question a law enforcement leader evaluating cloud services must consider is how much storage will the agency need? Are the pictures the agency wants to upload evidence or crime scene related? Are the videos from body cameras, in-car dash cameras, witness and subject interviews, detention and security videos, or commercial videos acquired as evidence? All these take up an excessive amount of storage and while the monthly storage costs and the cost of uploading the data may be low, what will it cost to access and download the data? There are numerous stories of cell providers "throttling" their digital use for users who are utilizing what is believed to be large amounts of bandwidth. Will the cloud services vendor do this to its customers? Is law enforcement access prioritized over that of other lower-priority municipal users, who might not be operational during a disaster or bad weather?

Storage considerations must also address the physical location where the data are maintained, as well as who can access the data. Yes, data are stored with the vendor, but where, physically, will data be managed? If the data are evidence, was that evidence kept in the United States? If not, will judges consider this a chain of custody issue? Who has access to the data or information? Law enforcement executives make significant efforts to maintain the security of the data obtained and used within their departments; will the same be said about a department's chosen vendor? Will the provider testify in open court about its security protocols and share access logs to ensure the chain of custody? It is this level of trust that the public believes to held by law enforcement, and a law enforcement executive must feel the same about the vendor that is selected. It is for these reasons that law enforcement executives must take steps to ensure that they review any contracts.

Potential Infrastructure and System Upgrades

Law enforcement executives have become accustomed to adapting to evolving situations and being keenly aware of their surroundings. The same approach should be applied to evaluating cloud services. Yes, the cost of storage may be less than what it currently costs a municipality to maintain and operate the systems and networks it has, but what about the peripheral issues? Obtaining a new patrol car will not benefit anyone if the agency cannot afford to add the peripheral equipment (e.g., lights, sirens, radios, computers), nor will purchasing new software if existing hardware no longer works and there is no funding for replacement. When evaluating a decision to undertake a move to cloud storage, law enforcement executives should hold planning meetings with their respective IT partners to include discussions about related issues. For instance, internal wiring and connections may be adequate for a locally stored infrastructure, but not when large amounts of data need to move across networks, out of the department, and to the new cloud provider. Will all current software, programs, and equipment be compatible? These details might not seem significant—until a law enforcement executive finds the evidence control data system used by the agency is not able to operate correctly in the cloud environment, potentially costing the department significant funds to upgrade or change.

Data Redundancy and Recovery Issues

Recovery after a disaster, natural or humanmade, is a vital part of any executive's considerations. Careful evaluation of the provider's redundancy (where backup and primary storage will be located) and recovery (how often the data are backed up and what percentage will become lost if the data center experiences a failure or malware attack) is essential. Executives need to carefully evaluate vendors and ensure that secondary or alternative data centers where backups are stored are geographically distant. Maintaining geographically separated backup systems aids in preventing a provider from being unable to restore access after a major catastrophe, such as a hurricane, strikes an area. Secondary data centers located within even a tri-state or regional area can become inaccessible as the result of a hurricane or power grid failure. While an incident, such as a hurricane, tornado, or earthquake can interrupt access to an agency's data, once power and connectivity are restored to the agency, the data should be available from the secondary location immediately, allowing access to vital records and continued agency operations. Law enforcement executives need to remember that their emergency and disaster planning, operational continuity planning, and recovery and remediation planning will need to be evaluated as part of this process and ensure that the restoration and the risk management portion of any contract receive adequate scrutiny.

Proprietary Cloud Considerations

Law enforcement executives will get a great deal of information from all kinds of providers, including, but not limited to Amazon, Google, Microsoft, and Axon. Storage by itself is a great value, but evaluation needs to be made to ensure the data are owned by the agency and the taxpayers who pay for it. If the technology placing the data in the cloud is proprietary, what happens if there is a vendor change? What happens if there is a budget disaster and the agency can no longer afford the storage? How does the agency then access its valuable data? These discussions should include the law enforcement executive, legal counsel, and IT staff. Due diligence, including how the law enforcement executive agency's data are classified and maintained, is essential. It is vital that when contracting with a proprietary cloud vendor, the law enforcement executive give careful consideration to the ownership and protection of the agency's information.

Summary

Law enforcement executives, no matter the size of their departments, undertake critical decisions and evaluate complex issues daily, and the implementation of technology that might save funding is always of interest. However, it is essential that the consideration of such technology options be complete—that all sides and all angles be evaluated and carefully considered. Evaluating the proposal to move to cloud services is another reason to ensure that existing plans include a proper external test of security and the existence of an accurate incident response plan.

Caution is paramount during the evaluation of such implementations. Once law enforcement executives understand the need for caution and ensure careful evaluation, they will be able to determine if modernization, to include moving to a cloud environment, is appropriate for their agencies. As with all travels, safely driving the information technology highway requires recognizing conditions and not moving faster than the driver can react. ❖

To aid law enforcement executives in reviewing security (for cloud or traditional IT services) and identifying related issues for consideration, the IACP created the *Cyber Report Card,* which is available, with additional resources, at the IACP Law Enforcement Cyber Center (**www.IACPcybercenter.org**).

Notes:

[1]*Techopedia*, s.v. "cloud storage," https://www.techopedia.com/definition/26535/cloud-storage.

[2]Sharon Stolting, Shawn M. Barrett, and David Kurz, *Best Practices Guide: Acquisition of New Technology* (International Association of Chiefs of Police), http://www.theiacp.org/portals/0/pdfs/BP-NewTechnology.pdf.

[3]International Association of Chiefs of Police (IACP), *IACP Technology Policy Framework* (Alexandria, VA: IACP, 2014), http://www.theiacp.org/Portals/0/documents/pdfs/IACP%20Technology%20Policy%20Framework%20January%202014%20Final.pdf.

Congratulations to
Southern Police Institute Alumni Association's

2018 Alumnus of the Year

Deputy Inspector (Ret.)
New York Police Department
Kevin G. Collins
110th AOC
SPIAA President 2007-2008

Come help us celebrate
at the
67th SPIAA
Annual Training Conference
in Concord, NC, July 9 - 12, 2018

For conference details, visit:
spiaa.org

The University of Louisville is an equal opportunity institution. This publication was prepared by the University of Louisville and printed with state funds KRS 57.375

IACP THROUGH THE YEARS

1999

The Evolution of the Computer Hacker's Motives

By Matthias A. Joyce, CISSP, Information Security Engineer, Litton/TASC, Chantilly, Virginia, and Lieutenant Shawn Barrett, Fairfax County Police Department, Fairfax, Virginia

In celebration of IACP's 125th anniversary, each 2018 issue of Police Chief *includes a republished article from the magazine's history, which dates back to 1934. The following article is from the February 1999* Police Chief.

Although the world of the computer "hacker" has been shrouded in mystery and myth, it is becoming increasingly important that law enforcement officials at all levels understand more about the evolution of this criminal behavior. Since the tools used by computer hackers are freely available and "user friendly," providing everyone the opportunity to become a hacker, law enforcement officers must be aware of the changes in computer hacker techniques, tools and motivations, as well as the personal characteristics of these criminals.

One of the confusing areas associated with computer hacking is the unique vocabulary or jargon used by the hacker community. The box on the next page presents definitions of selected terms to provide a common understanding for the rest of this article. Developed by John Howard,[1] who based his research on his work with the Computer Emergency Response Team at Carnegie Mellon University, these definitions have been modified by the authors in some cases to make them a little less technical.

The Hacker's Profile

Although the profiles posted on Phrack Inc.'s Web site[2] represent only a small fraction of actual computer hackers, they do encompass the more well-known members of the computer underground. The typical hacker, according to Phrack, is a white male, aged 15 to 34, who began using the computer underground between the ages of 10 and 25.

Jim Christy, a recognized authority on computer hackers, provides a deeper insight into the world of hackers, examining such characteristics as average hours per week involved with computer crime (11.7), average number of victims (154.2), average age when introduced to computers (9.5 years) and average age when introduced to computer crime (15 years). Taken together, these profiles describe the typical computer hacker as a young, white male.

Howard takes a process-oriented view of computer hacking, beginning with the attacker. With the hacking tools and methods that are readily available on the Internet—many of which require little technical expertise—hackers access others' computers to accomplish some desired objective. This may involve stealing information, launching attacks on other computer systems or simply exploring the target computer system. The motivation behind these objectives is the central theme of this article.

The Evolution of the Hacker's Motives

What motivates hackers to do what they do? How have these motives changed over time? What will motivate hackers in the future?

The earliest use of the term "hacker" applied to computer enthusiasts at the Massachusetts Institute of Technology, who were known to work around the clock—sometimes for 72 hours straight—attempting to perfect a computer program. The motivation for these hackers was the quest for knowledge of a new and emerging

technology—computers. These hackers literally built computers and spent countless hours exploring and documenting their capabilities and limitations. They challenged one another to develop innovative and creative solutions to problems.

The development of computers and computer operating systems was rapid. One of the first major developments in the computer field was the introduction of the UNIX operating system in 1969 at Bell Labs, the research division of AT&T.[3] Complex and not easily understood by casual users, the UNIX operating system was intended to breed an exclusive fraternity of technical people who really understood how to use it.

Early computer hackers were quick to adopt UNIX for two reasons: its flexible, unsecure architecture and its ready availability in the academic community.

UNIX allowed primitive computer procedures to be integrated to create complex computer applications. Using these primitive procedures as building blocks, system programmers could build complex applications with many different approaches and configurations. UNIX's flexibility enabled early hackers to solve problems in many innovative and creative ways. In addition, because it was designed to be used in a trusted environment, UNIX was not designed with sophisticated security measures.

Because it had been developed by Bell Labs, whose parent company—AT&T—was prohibited from selling software in the computer industry, UNIX was given away freely to academic institutions. Designed to satisfy the needs of a multi-user operating system, UNIX quickly took hold in university settings, where hackers tended to be more prevalent.

The knowledge sought by early hackers was primarily functional in nature; they wanted to understand the system's capabilities and limitations. Hackers spent endless hours testing and pushing UNIX computers to the limits of their performance, often identifying security vulnerabilities in the UNIX operating system in the process. Meticulously documented, these vulnerabilities soon became widely known among other hackers.

Although most of the hackers who worked to identify UNIX vulnerabilities still held to the principles of academic research and, therefore, did not purposely cause damage to the computer systems or data files, not all of the newer hackers adhered to the same principles. For these renegade hackers, the thrill and challenge of breaking into computer systems was their driving motivation.

Breaking into computer systems motivates malicious hackers because it provides an ego-boosting sense of power and control.

A Hacker's Glossary

While specific meanings may vary among hackers, these are generally accepted computer hacker terms.

Back door: A designed mechanism that enables a perpetrator to circumvent the security measures of a computer system.

Crack: A common hacker program to reverse-engineer computer passwords.

Denial-of-service: The intentional degradation or blocking of computer or network resources.

Dumpster diving: Searching for passwords or other sensitive information in the trash.

E-mail: Electronic mail.

FTP: File Transfer Protocol—a program to transfer files between computers on a network.

Hacker: An individual who breaks into computers primarily for the challenge and status.

Logic bomb: A piece of software code that executes when a predetermined event occurs. For example, if a certain name did not appear in the payroll system, the logic bomb would delete the payroll database.

Root: A user with root-level privilege, who has the ability to perform any actions on a UNIX-based computer system—create user accounts, delete or modify files, or stop applications.

Script: A text file that contains a sequence of computer commands. Hackers use scripts to reduce the possibility of typing errors when entering computer commands.

Sendmail: A common electronic mail application in UNIX environments.

Sniffer: A program to monitor and record all data sent over a computer network.

TCP/IP: Transmission Control Protocol/Internet Protocol—the suite of telecommunication protocols that govern the transmission of data on the Internet.

Time bomb: A logic bomb whose predetermined event is time-based.

Toolkit: A software package containing scripts, programs and autonomous agents that allow a hacker to exploit the vulnerabilities of a specific computer system. Toolkits for various computer systems are readily available on the Internet, and hackers uses them to penetrate specific computer systems.

Trojan horse: A program that performs like a real program a user may wish to run, but also performs unauthorized actions. For example, the computer log-on process could log on a user, but also record the user's identification and password.

UNIX: An operating system developed by Ken Thompson and Dennis Ritchie in 1969. It is the predominant operating system used in universities and critical business processes.

These hackers often boast of their exploits, which may be chronicled in a number of underground publications.[4] This new breed of hacker leverages the knowledge accumulated by earlier hackers over countless hours and uses it to break into various computer systems for malicious purposes. Having strayed from the original principles of the first hackers, the newer hackers became disenfranchised and developed a new subculture, focused on breaking into systems, that has proven very attractive to younger computer enthusiasts.

Although many of the newer hackers caused problems in systems they accessed by virtue of their *lack* of expertise in the operation and use of the UNIX operating system, Kevin Mitnick is one of the new breed who used his expertise to cause extensive damage, including erasing several of U.S. Leasing's critical business files.[5] When the system administrator noticed that critical files had been altered or deleted, and application programs had been used without authorization, he began to implement various computer security measures, such as passwords, to restrict the hacker's access and protect the integrity of the system.

Thus began a cycle of one-upmanship between the system administrator and the hacker. As the system administrator implemented better security mechanisms to restrict the hacker's access, the hacker developed more innovative methods to defeat the new security measures. The system administrator's actions actually provided the hacker with new challenges to motivate him. For example, Mitnick used social engineering techniques to convince unsuspecting system administrators or users to provide him with valid user IDs and passwords. These passwords gave Mitnick valid access to the system, thus circumventing the password security measures.

The cat-and-mouse game between hackers and system administrators is the motivation that currently drives most of today's hackers. But there are several factors that may change the motivation for computer hackers in the future.

The increased globalization of the world's economies, integration of information technology into critical business processes and corporate embrace of the Internet can all be expected to significantly alter hackers' motivation and behavior.

Instead of breaking into computer systems for the thrill and status, hackers may use their skills for political or financial gain. The case of Vladimir Levin is a chilling example of this disturbing trend.

In 1994, Vladimir Levin, a 28-year-old hacker from St. Petersburg, Russia, stole millions of dollars from Citibank's cash-management system in New York City.[6] Although most of the stolen funds were eventually recovered, the Levin case presents several troubling considerations for law enforcement. First, Levin performed all of his activities from a country other than that where the bank was located. The Internet's ability to make physical distance irrelevant causes many problems for law enforcement. Where did Levin's crime take place? St. Petersburg or New York City? Who has jurisdiction? The size of the theft is also troubling. In a traditional bank robbery, the thief may be able to steal a few thousand dollars, but a cyber thief can easily steal millions of dollars. If a cyber crook were able to skim .01 percent of the trillions of dollars transferred electronically each day, he would have a $100,000-a-day job. Finally, the Citibank case is rare because it was reported.

The majority of hacker attacks that result in financial loss go unreported. There appear to be several reasons why financial organizations are reluctant to report cyber crime, but chief among them is the potential loss of the public's trust in the financial institution. Would anyone willingly keep his hard-earned money in a bank that cannot protect it from cyber crooks?

The cat-and-mouse game between hackers and system administrators is the motivation that currently drives most of today's hackers.

In addition to the financial motivation, future hackers may apply their skills for political or social reasons. The recent attack on the Nation of Islam's Web page, in which derogatory text was inserted on the page two days after the Million-Man March, is a good example of a politically motivated attack.[7] The Department of Justice's Web page was also recently attacked, in response to DOJ's support of the Communications Decency Act.

Because of the fierce competitive pressures in today's global marketplace, economic espionage is an increasing reality for U.S. business.[8] More than 50 countries, both friendly and unfriendly to the United States, actively use hacker tools and techniques to improve their industries' competitive advantages. It is not inconceivable that hackers will one day offer their services to foreign governments trying to assist their nation's industries. In fact, several nations are redirecting their existing espionage activities to target businesses and industries in the United States.

Conclusion

Although it is not a new activity, computer hacking is a different crime today than it once was, with motivations that have evolved as the technology has matured. While it may have begun as a quest for knowledge, hacking at the end of the 20th century is a clearly criminal activity, often conducted for political or financial gain. To combat this threat, law enforcement officials will need to become better versed in hackers' tools, techniques and motivations. ❖

Notes:

[1]John D. Howard, "An Analysis of Security Incidents on the Internet 1989-1995," Dissertation, Carnegie Mellon University, Pittsburgh, Pennsylvania, April 7, 1997.

[2]*Phrack Inc. Magazine*, http://www.phrack.com.

[3]"History of UNIX," http://www.dcs.warwick.ac.uk/-carters/Eudid_UNlX/1_2_2.html, as viewed 3/16/98.

[4]*Phrack Inc. Magazine*, http://www.phrack.com; *2600[*end[, http://www.2600.com; "Blacklisted!" *411*, Syntel Vista, Inc.

[5]Katie Hafner and John Markoff, "Cyberpunk," *Touchstone*, 1991, p. 33.

[6]Joseph L. McCarthy, "Cyberswindle!" *Chief Executive* (U.S.), May 1996, p. 38.

[7]Sewell Chan, "Electronic Vandals Tamper with Web Pages," *Wall Street Journal*, June 26, 1996.

[8]Frank Swoboda, "Economic Espionage Rising, FBI Director Tells Congress," *The Washington Post*, February 29, 1996.

IACP Through the Years article reprints reflect the eras in which they were first published and should not be construed as necessarily reflecting the IACP's current view or stance on topics.

Coming next month:

"Guam, USA: The New Drug Mecca" by Kenneth E. North, taken from the April 1979 edition of *Police Chief*.

APPLICATIONS ARE NOW BEING ACCEPTED

The IACP/Target Police Officer of the Year Award is an opportunity to recognize heroes who work tirelessly every day to make communities safer.

Nominations are now being accepted to honor exceptional achievements in any police endeavor. Achievements include but are not limited to extraordinary valor, crime prevention, investigative work, community relations, traffic safety, drug control and prevention, juvenile programs, and training efforts.

Four finalists will be chosen and each will receive:

- A trip to IACP 2018, in Orlando, Florida including airfare, hotel, conference registration, and stipend for the nominee and a guest.
- Recognition at the IACP Foundation Gala, where one finalist will receive the Police Officer of the Year Award.
- Recognition of the Police Officer of the Year at the General Assembly.
- Feature in *Police Chief Magazine*.

The IACP is proud to partner with Target to continue this tradition of recognizing the exemplary performance by law enforcement from across the globe.

Please join us in helping honor and recognize these everyday heroes.

THE IACP FOUNDATION
Never Feel Abandoned

APPLICATION DEADLINE: FRIDAY, JUNE 22, 2018

For eligibility information and a nomination form please visit: **www.theIACP.org/POY**

For questions, please contact **awards@theiacp.org**

IACP
International Association of Chiefs of Police
125 Years
1893 - 2018

Participate in the 2018

MEMBER•TO•MEMBER DRIVE!

Runs February 1 to June 30, 2018

- CONNECT
- PARTICIPATE
- LEARN
- ADVOCATE
- SUCCEED

BRING IN NEW MEMBERS AND WIN PRIZES!

You know the value of IACP membership. Share the benefits with others by encouraging them to join as new members.

In honor of **IACP's 125th Anniversary** — Every member is encouraged to recommend new members to join and be rewarded for your efforts.

Membership in the IACP is open to EVERYONE involved in criminal justice – both sworn and civilian.

Recommend one new member and receive an official **IACP gift***.

Recommend 5 new members and receive a free registration to the **2018 IACP Annual Conference and Exposition**, October 6 - 9, 2018, in Orlando, Florida, USA. (a $425 value!)

THE IACP

Serving the Leaders of Today and Developing the Leaders of Tomorrow®

2018 MEMBER-TO-MEMBER DRIVE RULES AND INFORMATION:

1. In order to qualify for prizes, new members must use the 2018 Member-to-Member Membership Drive application. Photocopies are acceptable.
2. Applications must be received at IACP Headquarters by the **close of business June 30, 2018**.
3. Renewing members do not qualify for this drive.
4. Prizes are non-transferable.
5. Members will be sent/notified of all prizes and incentives following the conclusion of the drive.
6. *The first 250 members to sponsor a new member in the drive will receive the official IACP gift. The item sent will be at the discretion of the IACP.

IACP Member-To-Member Drive Application

International Association of Chiefs of Police
P.O. Box 62564
Baltimore, MD 21264-2564, USA
PHONE 1.800.THE IACP • 703.836.6767 • FAX 703.836.4543
theIACP.org

DO NOT USE

Name:_____ _____ _____ (*Please Print*)
First Middle Initial Last

Title/Rank: _____

Agency/Business Name: _____

Business Address:_____

City, State, Zip, Country:_____

Residence Address: _____

City, State, Zip, Country:_____

Business Phone:_____ Fax:_____

Send mail to my ❑ Business ❑ Residence Address

E-mail: _____

Website: _____

Have you previously been a member of IACP? ❑ Yes ❑ No

Date of Birth: (MM/DD/Year) _____/_____/_____ I am a sworn officer. ❑ Yes ❑ No

Number of sworn officers in your agency (*if applicable*) ❑ a. 1–5 ❑ b. 6–15 ❑ c. 16–25
❑ d. 26–49 ❑ e. 50–99 ❑ f. 100–249 ❑ g. 250–499 ❑ h. 500–999 ❑ i. 1000+

Approximate pop. served (*if applicable*) ❑ a. under 2,500 ❑ b. 2,500–9,999 ❑ c. 10,000–49,999
❑ d. 50,000–99,999 ❑ e. 100,000–249,999 ❑ f. 250,000–499,999 ❑ g. 500,000 +

Education (*Highest Degree*):_____

Date elected or appointed to present position: _____

Law enforcement experience (*with approx. dates*): _____

_____

❑ I am recommended for membership by: _____

Amount to be charged _____ (*U.S. dollars only* – Membership includes subscription to *Police Chief* magazine *valued at $30.*)

I have enclosed: ❑ Purchase order ❑ Personal check/money order ❑ Agency check
Charge to: ❑ MasterCard ❑ VISA ❑ American Express ❑ Discover

Cardholder's Name: _____

Card #:_____ Exp. Date: _____/_____

Cardholder's Billing Address: _____

Signature:_____

All memberships expire December 31 of each calendar year. Applications received after August 1 will expire the following year. Return completed application via mail, fax (703-836-4543) or email (membership@theiacp.org). Questions? Contact Membership at 800-THE-IACP.

M2M18

Membership Categories

Information on membership categories, benefits, and eligibility can be found on the IACP web site **www.theiacp.org/membership**

❑ Active Member (*sworn command level*) $150

Associate Member:

❑ General $150
❑ Academic $150
❑ Service Provider $250
❑ Sworn Officer—Leader of Tomorrow (*sworn non-command level*) $75
❑ Student—Leader of Tomorrow University name: $30

Optional Section Memberships:

❑ Capitol Police Section $30
❑ Defense Chiefs of Police Section $15
❑ Drug Recognition Expert (DRE) $25
❑ Indian Country Law Enforcement $25
❑ Intl Managers Police Academy & College Training $25
❑ Law Enforcement Information Management (LEIM) $25
❑ Legal Officers $35
❑ Mid-Sized Agencies Section $50
❑ Police Foundations Section $20
❑ Police Physicians $35
❑ Police Psychological Services—initial processing fee $50
❑ Public Information Officers $15
❑ Public Transit Police No Charge
❑ Railroad Police No Charge
❑ Retired Chiefs of Police No Charge
❑ Smaller Department Section $20
❑ S & P Police Alumni Section No Charge
❑ S & P Police Academy Directors No Charge
❑ S & P Police Planning Officers No Charge
❑ University/College Police—Initial Member $50
❑ University/College Police—Additional members $15

NEW MEMBERS

This posting of new member applications is published pursuant to the provisions of the IACP Constitution & Rules. If any active member in good standing objects to any application, written notice of the objection must be submitted to the executive director within 60 days of publication. The application in question shall then be submitted to the Executive Committee and shall require the affirmative vote of two-thirds of the members of that committee for admission of the applicant.

The full membership listing can be found in the members-only area of the IACP website (www.theiacp.org).

Contact information for all members can be found online in the members-only IACP Membership Directory.

*Associate Members
All other listings are active members.

ENGLAND

Wilmslow
*Prasad, Yogesh, Senior Manager, Thermo Fisher Scientific

INDIA

Naya Raipur
Shaikh, Arif, Superintendent of Police, Chhattisgarh Police Service

NIGERIA

Enugu
*Mashat, Sylvanus Danladi, Police Officer, Nigeria Police Force

Ibadan
*Adeyefa, Ademola Michael, Sergeant, Nigeria Police Force
Ajisebutu, Adekunle, Superintendent of Police, Nigeria Police Force

Ikare-Akoko
Micheal, Ogundola Olamide, Assistant Superintendent of Police, Nigeria Police Force
Oluwafemi, Akinyeye Samuel, Assistant Superintendent of Police, Nigeria Police Force

Onikan
*Titilayo, Abiodun Olatunbosun, Inspector of Police, Nigeria Police Force

Shomolu
Akinlabi, Lasisi Adeolu, Assistant Superintendent of Police, Nigeria Police Force

UNITED STATES

Alabama

Birmingham
*Harper, Curt E, Chief Toxicologist/DRE Instructor, Alabama Dept of Forensic Sciences

Decatur
*Hannah, Seth M, State Trooper, Alabama Law Enforcement Agency
*Smith, Eric, Senior Trooper, Alabama Law Enforcement Agency

Dothan
*Owens, Michael S, Sergeant, Dothan Police Dept

Helena
Flynn, William Brad, Lieutenant, Helena Police Dept

Huntsville
*Nelson, Michael J, Police Officer, Huntsville Police Dept

Mobile
*Bogle, John Daryl, Sergeant, Alabama State Trooper, Post Commander, Alabama Law Enforcement Agency

Opelika
*Mayo, David C, DRE/Patrol Sergeant, Lee Co Sheriff's Office

Orange Beach
Simonson, John J, Lieutenant, Orange Beach Police Dept

Arizona

Gilbert
Rodriquez, Joe, Commander, Gilbert Police Dept

Arkansas

Green Forest
Bailey, John L, Chief of Police, Green Forest Police Dept

California

Banning
Gil, Radames, Chief of Tribal Police, Morongo Band of Mission Indians

Carmel
Tomasi, Paul, Chief of Police, Carmel-by-the-Sea Police Dept

Chula Vista
Nighswonger, Davis W, Chief of Police, Southwestern College Police Dept

El Cajon
*Larson, Jeremiah J, Sergeant, El Cajon Police Dept
*MacArthur, Keith W, Sergeant, El Cajon Police Dept

Pleasant Hill
Hill, Bryan, Chief of Police, Pleasant Hill Police Dept

Redlands
*Strobaugh, Eric, Police Officer, Redlands Police Dept

Warner Springs
Monahan, Brian K, Chief of Tribal Police, Los Coyotes Police Dept

Colorado

Fort Collins
*Workman, Carol, Acting Director Information Services, Fort Collins Police Service

Connecticut

Southington
Palmieri, William, Deputy Chief of Police, Southington Police Dept

Wolcott
*Gugliotti, Michael, Owner/Managing Member, Under the Sun Investigations LLC

Delaware

Dover
Aydelotte, Drew T, Chief Fish & Wildlife, Delaware Natural Resources Police

District of Columbia

Washington
Hacker, J C, Deputy Assistant Director, FBI Criminal Investigative Division
*Jarvis, Elise M, Asst Director LE Outreach, Anti Defamation League
*Korinek, Frank W, Director Spectrum & Regulatory Govt Affairs, Motorola Solutions Inc

*Reza, Sara, Program Coordinator, US Holocaust Memorial Museum

Florida

Coral Springs
Irwin, Gerald, Captain, Coral Springs Police Dept

Orlando
*Parlapiano, David, Licensed Psychologist, David M Parlapiano Psyd LLC

Georgia

Chamblee
Waasdorp, Jason, Assistant CID Commander, Chamblee Police Dept

Dublin
Chatman, Anthony T, Chief of Police, Dublin Police Dept

Jonesboro
Busch, Brian, Chief Investigator, Clayton Co Office of the District Attorney

McDonough
*Palmer, Kenneth, Police Officer, Henry Co Police Dept

Illinois

Antioch
Johnson, Norman, Commander, Antioch Police Dept

Champaign
Shaffer, David, Deputy Chief of Police, Champaign Police Dept

Chicago
Riggio, Paul T, Deputy Chief of Police, Metra Police Dept

Cicero
Dimmick, Charles, Deputy Chief of Police, BNSF Railway Police Dept

Hillside
Lukaszek, Joseph M, Chief of Police, Hillside Police Dept

Hoopeston
DeWitt, James L, Chief of Police, Hoopeston Police Dept

Kankakee
Bertrand-Essington, Bridget, Major, Kankakee Community College

South Holland
Staples, Shawn, Chief of Police, South Holland Police Dept

Yorkville
*Richardson, Bobby J, Sergeant, Kendall Co Sheriff's Office

Kansas

Hutchinson
*Gould, Ron, Assistant Director, Kansas Law Enforcement Training Center

Lenexa
Schmitz, Eric, Captain, Lenexa Police Dept

Salina
Payne, Matthew B, Lieutenant, Kansas Hwy Patrol

Kentucky

Campbellsville
*Perian, Scotty R, Sergeant, Campbellsville Police Dept
*Wilson, Michael Shannon, Sergeant, Campbellsville Police Dept

Frankfort
Medley, Jeff, Lieutenant Colonel, Kentucky State Police

Louisiana

Many
Freeman, Roger, Chief of Police, Many Police Dept

New Orleans
*Coco, Jennifer, Associate, Bizer & Dereus LLC

Opelousas
Leblanc, Graig, Lieutenant, Opelousas Police Dept

Maryland

Baltimore
*Cokley, Tankeisha, Police Officer, Baltimore Police Dept
*Matthews, Emma, Student, Univ of Baltimore
*White-Bey, Aisha, Police Officer, Baltimore Police Dept

College Park
*Marsh, Kris, Associate Professor, Univ of Maryland Dept of Sociology

Gaithersburg
*Almiggabber, Sherif, Police Officer, Montgomery Co Police Dept

Silver Spring
*Wilcher, Edward D, Sergeant, Montgomery Co Police Dept

Massachusetts

Boston
Shuman, Samuel K, Chief, Federal Reserve Police

Edgartown
McNamee, Bruce, Chief of Police, Edgartown Police Dept

Plymouth
Petersen, Scott, Assistant Superintendent, Plymouth Co Sheriff's Office

Weymouth
Perchard, John, Detective Lieutenant, Weymouth Police Dept

Michigan

Grand Rapids
*Rewa, Kristen, Assistant City Attorney/Police Legal Advisor, City of Grand Rapids

New Baltimore
Riebel, Fred A, Chief of Police, New Baltimore Police Dept

Minnesota

Clara City
Wood, Kimberly M, Chief of Police, Clara City Police Dept

La Crescent
Stavenau, Douglas J, Chief of Police, La Crescent Police Dept

Minneapolis
*Veliz, Gio, Lieutenant, Minneapolis Police Dept

Savage
Gordon, Scott J, Captain, Savage Police Dept

St Louis Park
Garland, Mikael, Lieutenant, St Louis Park Police Dept

Stillwater
Starry, Dan E, Sheriff, Washington Co Sheriff's Office

Woodbury
*Bauer, Neil, Sergeant, Woodbury Police Dept

Mississippi

Fayette
McMiller, LaShawn, Chief of Police, Fayette Police Dept

Long Beach
McRight, Damian S, Commander Support Services, Long Beach Police Dept

Pascagoula
Ezell, Mike, Sheriff, Jackson Co Sheriff's Office

Missouri

Hillsboro
Hutt, John S, Lieutenant/Acting Chief of Police, Hillsboro Police Dept

Kirkwood
Raymond, Douglas M, Lieutenant, Kirkwood Police Dept

New Jersey

Camden
*Smith, Aaron G, Sergeant, New Jersey State Parole Board

Lawrence Township
*Bloom, Elliot, Senior Director, Taft Communications

New Mexico

Albuquerque
Wade, Terry, Special Agent in Charge, FBI

Lovington
Martinez, Jon, Chief Deputy, Lea Co Sheriff's Office

New York

Albany
Clapper, Jeremy W, Inspector, New York State Univ Police

Perry
Grover, Michael J, Chief of Police, Perry Police Dept

Plattsburgh
Ritter, Levi, Chief of Police, Plattsburgh Police Dept

Port Washington
*DeMasco, Sheryl, IT Specialist, Port Washington Police District

Ravena
Contento, Daniel, Acting Chief of Police, Coeymans Town Police Dept

Waterloo
Godley, Jason E, Chief of Police, Waterloo Village Police Dept

North Carolina

Dunn
West, Charles, Chief of Police, Dunn Police Dept

Forest City
Hensley, Donnie E, Captain, Forest City Police Dept

Ohio

Berea
Hedinger, Joseph, Lieutenant, Berea Police Dept

Dayton
Dickey, Matthew, Lieutenant, Dayton Police Dept

Middleburg Heights
Tomba, Edward J, Chief of Police, Middleburg Heights Police Dept

Oxford
Fening, Lara L, Lieutenant, Oxford Division of Police

Put-in-Bay
Riddle, Paul S, Chief of Police, Put-in-Bay Police Dept

Oregon

Bend
Maniscalco, Jason, Detective Lieutenant, Bend Police Dept

Prineville
Gautney, John W, Sheriff, Crook Co Sheriff's Office

Talent
Snook, Jennifer, Lieutenant, Talent Police Dept

Pennsylvania

Erie
Mook, Carter L, Captain, Millcreek Twp Police Dept

Laureldale
Carr, Felix E, Chief of Police, Laureldale Borough Police Dept

South Carolina

Conway
Long, Clayton D, Chief of Police, Conway Police Dept

Tennessee

Lebanon
Justice, Michael W, Chief of Police, Lebanon Police Dept

Murfreesboro
Williams, Clayton, Lieutenant, Murfreesboro Police Dept

Texas

Argyle
Cottle, Temple, Chief of Police, Argyle Police Dept

Arlington
McGrath, John P, Training Center Commander/Lieutenant, Arlington Police Dept

Austin
Davis, Kevin R, Chief of Staff, Texas Parks & Wildlife Dept

Beeville
Bridge, Robert J, Chief of Police, Beeville Police Dept

Fort Worth
Jones, Michael, SSA RPT Training and Development, BNSF Railway Police Dept
Longman, Jeff, Deputy Chief of Police, BNSF Railway Police Dept
*Morgan, Wayne, Senior Manager Safety and Training, BNSF Railway

Frisco
Crawford, Mike, Lieutenant, Frisco Police Dept

Galveston
Davis, Peter, Chief of Police, Galveston Park Board of Trustees Police Dept

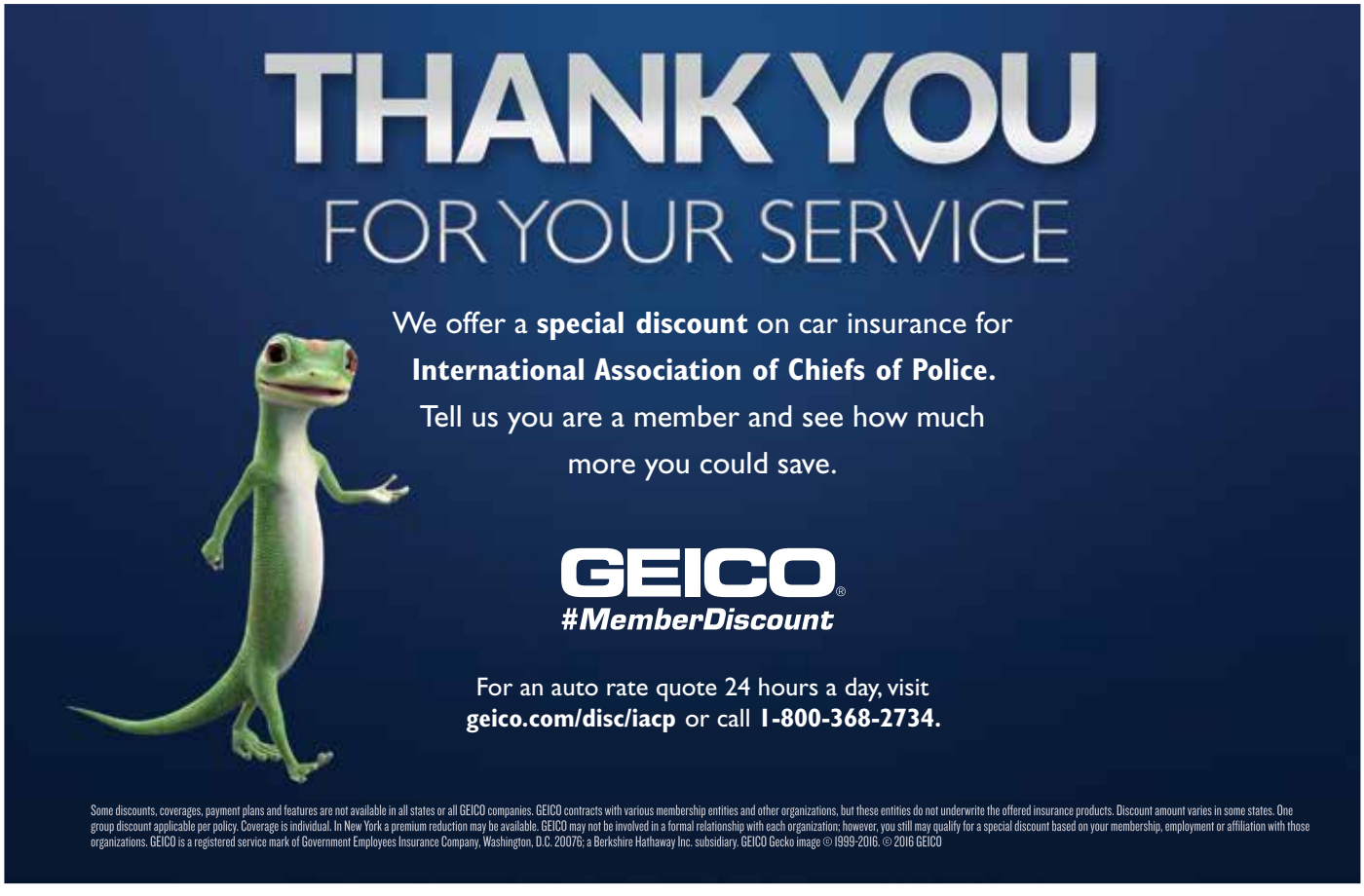
League City
Spencer, James, Assistant Chief of Police, League City Police Dept

San Antonio
*Lindley, Cynthia K, Patrolman, San Antonio Police Dept
Tijerina, Don, Chief Deputy, Bexar Co Sheriff's Office

Texas City
Stanton, Joe, Assistant Chief of Police, Texas City Police Dept

Utah

Richfield
Lloyd, Trent, Chief of Police, Richfield Police Dept



Springdale
Ray, J J, Lieutenant, Springdale/Zion Canyon Dept of Public Safety

Vermont

Shelburne
Noble, Aaron S, Chief of Police, Shelburne Police Dept

Virginia

Alexandria
*Golden, Raymond F, Police Officer, Alexandria Police Dept
*Wortham, Carl, Officer, Alexandria Police Dept

Arlington
Medina, Rafael, Deputy Asst IG-Investigations & Analytics, US Postal Service OIG

Berryville
Sumption, Travis, Chief Deputy, Clarke Co Sheriff's Office

Virginia Beach
*Hughes, Chase, President, Ellipsis Behavior Laboratories

Washington

Seattle
Johanknecht, Mitzi G, Sheriff, King Co Sheriff's Office

Spokane
*Carpenter, Paul, Sergeant, Spokane Police Dept

Wisconsin

Eagle
Duran, Gregg R, Chief of Police, Eagle Police Dept

The IACP notes the passing of the following association members with deepest regret and extends its sympathy to their families and coworkers left to carry on without them.

Paul D. Cobb, Chief of Police (ret.), Pasadena, Texas

Rick J. Townsend, Chief of Police, Adairsville, Georgia

REMEMBER: Law enforcement professionals at every level qualify for membership in the IACP.

CENTER FOR OFFICER SAFETY & WELLNESS
IACP

Line of Duty Deaths

"They will be remembered—not for the way they died, but for how they lived."

The IACP wishes to acknowledge the following officers, who made the ultimate sacrifice for their communities and the people they served. We extend our prayers and deepest sympathies to their families, friends, and colleagues.

Corporal Dale Hallman
Saluda County Sheriff's Office, South Carolina
Date of Death: April 6, 2018
Length of Service: 5 years

Police Officer Keith Erle
Huntsville Police Department, Alabama
Date of Death: April 9, 2018
Length of Service: 26 years

Patrolman Kevin Crossley
Whitesboro Police Department, New York
Date of Death: April 11, 2018
Length of Service: 8 years

Police Officer Sean Gannon
Yarmouth Police Department, Massachusetts
Date of Death: April 12, 2018
Length of Service: 7 years, 5 months

Detective Sergeant Brian Cuscino
New Castle Police Department, Pennsylvania
Date of Death: April 19, 2018
Length of Service: 17 years

Deputy Sheriff Taylor Lindsey
Gilchrest County Sheriff's Office, Florida
Date of Death: April 19, 2018
Length of Service: 2 years

Sergeant Noel Ramirez
Gilchrist County Sheriff's Office, Florida
Date of Death: April 19, 2018
Length of Service: 7 years

Deputy Sheriff Casey Shoemate
Miller County Sheriff's Office, Missouri
Date of Death: April 20, 2018
Length of Service: 1 year (with agency)

Police Officer Tamby Yagan
Paterson Police Department, New Jersey
Date of Death: April 22, 2018
Length of Service: 13 years

Master Deputy James Kirk, Jr.
Lancaster County Sheriff's Office, South Carolina
Date of Death: April 24, 2018
Length of Service: 28 years

Corporal Eugene Cole
Somerset County Sheriff's Office, Maine
Date of Death: April 25, 2018
Length of Service: 13 years

Police Officer Rogelio Santander, Jr.
Dallas Police Department, Texas
Date of Death: April 25, 2018
Length of Service: 3 years

Police Officer Jesus Cordova
Nogales Police Department, Arizona
Date of Death: April 27, 2018
Length of Service: 11 years

Police Officer Charles Whites
Round Rock Police Department, Texas
Date of Death: April 27, 2018
Length of Service: 19 years

Police Officer Rob Pitts
Terre Haute Police Department, Indiana
Date of Death: May 4, 2018
Length of Service: 16 years

Agent Joel Pantojas-Fuente
San Juan Police Department, Puerto Rico
Date of Death: May 6, 2018
Length of Service: 18 years

Product update

The **Police Chief** *keeps you on the cutting edge of law enforcement technology with monthly product announcements. For* ***free*** *in-depth information, visit us online at www.policechiefmagazine.org. Items about new or improved products are based on news releases supplied by manufacturers and distributors; IACP endorsement is in no way implied.*

Touchscreen displays for helicopter

Robinson has added Garmin's new G500H TXi displays to its R44 and R66 options. The two TXi displays add touchscreen functionality to Garmin's popular G500H system and consolidate PFD/MFD information onto a single screen. The upgraded displays provide increased resolution and interface with Garmin's GTN 6xx/7xx touchscreen GPS series. The new landscape-oriented display was designed specifically for Robinson and allows the pilot to switch between a full-screen PFD or full-screen moving map. The compact console configuration eliminates the need for a separate GTN GPS console in front of the pilot.

For more information, visit www.robinsonheli.com.

Voice biometrics engine

Phonexia launched Deep Embeddings, the latest generation of its voice biometrics engine for speaker identification and verification. The new technology uses deep neural networks (DNN) to map voices directly to their unique small and fixed-length records called voiceprints. Deep Embeddings is available within the Phonexia Speech Platform and is the world's first commercially available voice biometric engine with this machine learning capability. It uses a discriminative training model to identify the truly unique features in each individual's voice, creating voiceprints fast.

For more information, visit www.phonexia.com/en/product/voice-biometrics.

Intelligent video management solution

Arteco offers the Arteco Videowall, which enhances situational awareness and improves multiagency collaboration. Arteco Videowall delivers a rich experience by combining data, including videos, maps, peripherals, web pages, integrated third-party systems, and event notifications, into a single visual interface. Other specialized content, such as real-time news feeds, weather monitoring, system status information, and operator protocols, can be easily shared with others, facilitating joint and immediate action. Completely scalable, Videowall supports a wide variety of security operation centers. The solution can also be leveraged across multiple sites in different locations, such as a local emergency operations center.

For more information, visit www.arteco-global.com.

UAV data extraction tools

MSAB has partnered with URSA Inc. to expand its drone forensic capabilities. URSA's Idetic Unmanned tools are designed to collect, integrate, analyze, and present UAV-related data. The company provides accurate understanding of drone telemetry data and metadata to support law enforcement and intelligence investigations in the rapidly evolving unmanned vehicle and robotics ecosystem. MSAB's product XRY now supports extraction of data from a number of popular drone models, allowing investigators to see flight path data and other data that can assist their investigations and enforcement activities involving illegal drones.

For more information, visit www.msab.com/products/drones.

LEADERSHIP in POLICE ORGANIZATIONS℠

IACP's Leadership in Police Organizations (LPO), is modeled after the concept of "every officer is a leader" and is designed to enhance the leadership capacity of established supervisors. Attendees will gather with leaders from around the globe and grow their experience and knowledge with:

INTERACTIVE TRAINING FORMAT

APPLIED LEARNING

TRANSLATION OF THEORY TO PRACTICE

PRACTICAL LEADERSHIP STRATEGIES

Secure Your Space for Upcoming Training Opportunities

PLANO, TEXAS

2018

July 23-27 • August 20-24 • September 24-28

FIRST-LINE LEADERSHIP

The IACP's First-Line Leadership (FLL) training provides leadership and management skills to sergeants, corporals, master police officers, and other current and aspiring leaders. Training participants will:

- Enhance communication and manage change.
- Learn key themes of followership and motivation.
- Acquire leadership skills and risk management strategies.
- Learn to maneuver in political environments.
- Create community needs assessments.
- Address current critical policing issues.

BRING LEADERSHIP TRAINING TO YOUR AGENCY

Build the leadership capacity in your community and show dedication to your staff's professional development by hosting a training. For more information:

125 Years 1893 - 2018

IACP International Association of Chiefs of Police

LPOTeam@theIACP.org • theIACP.org/LPO

FirstLineLeadership@theIACP.org • theIACP.org/First-Line-Leadership

800.THE.IACP

In-vehicle cell signal boosters

SureCall, the performance leader for cellular signal boosters, announces the Fusion2Go 3.0 and Fusion2Go 3.0 RV, its newest generation of in-vehicle cell phone signal boosters. SureCall's products for commercial, personal, and fleet use, including the Fusion2Go line, boost cellular service in areas with critically low cell signal strength. The Fusion2Go 3.0 and Fusion2Go 3.0 RV boost all North American carrier signals to provide a car full of users with reliable voice, text, and 4G LTE data. The SureCall Fusion2Go line works with all cellular providers in the United States and Canada.

For more information, visit www.surecall.com.

Rifles

DoubleStar Corp., manufacturers of high-quality, U.S.-made AR components, rifles, and pistols, introduces the American-made STAR10-BX rifle line with two new calibers: 6.5 Creedmoor and .260 Remington. The STAR10-BX utilizes a 22-inch stainless steel, free floating, heavy barrel with a 1:8 twist rate for added velocity. It also incorporates the STAR10-B billet aircraft 7075 TC aluminum upper and lower receivers anodized to MIL-SPEC. The flattop upper receiver features a brass deflector and dust cover, while the lower receiver features an integrated trigger guard and enhanced magazine well. The STAR10-BX also features a CMC 3.5 lb. Trigger Group and the ACE Hammer buttstock.

For more information, visit www.star15.com.

Motion capture camera

Developers at Qualisys offer a new camera to the Oqus line. The Oqus 6+ is a high-end camera, suitable for traditional motion capture labs, but without the traditional high cost. Oqus cameras are daisy-chained, which means less cables and easier setup. IP67 hardware and covered housing protects the technology from wet and cold environmental conditions. By filling the void between too many high-end features and low cost, the Oqus 6+ is making the Oqus camera the most versatile in the motion capture industry.

For more information, visit www.qualisys.com.

Cellphone call data analytics updates

CellHawk from Hawk Analytics has new updates, such as reverse phone lookup—users can hover over and right-click any outside number within CellHawk to get the carrier and subscriber information within seconds. Hawk Analytics has integrated the case manager, agency account information, phone lookup tool, and content from Support@Hawk into its new dashboard concept. The improved preservation letter and search warrant templates have easy-to-use drop-down options. The advanced filtering tool offers more filtering options to one or all target records.

For more information, visit www.hawkanalytics.com.

High-visibility garments

West Chester Protective Gear is introducing a new line of high-quality, high-visibility garments, distinguished by a broad range of styles, customization options, and low price points. The product line includes vests, shirts, outerwear and rainwear, designed for a variety of work environments. All vests and shirts feature moisture wicking to keep wearers dry and comfortable. They are available in classic, breakaway, and surveyor styles with many color block and reflective tape patterns. Standard and oversized pockets allow wearers to store smaller cell phones, pens and notebooks, as well as larger tablet-sized electronics. Ladies' vest sizes are also offered.

For more information, visit westchestergear.com/vizup.

Smart technology for bike patrols

Ekin, the leader in safe city technologies, offers the Ekin Bike Patrol, the first and only smart patrol product for bicycles. It performs automatic license plate recognition (ALPR), speed detection, and parking violation detection on the move. It is easily installed on any police bicycle. The compact design allows for parking violation and speed detection and number plate recognition even at areas fixed solutions cannot control and where motored vehicles reach their limits. It detects vehicles that are on the blacklist by their number plates and generates an audio or visual alarm notification on its tablet application.

For more information, visit www.ekin.com

Video storage solution

StorageCraft is addressing the high cost, complexity, and compliance of storing video surveillance footage with an innovative solution that meets the storage demands of law enforcement surveillance. The number of police departments mandated to deploy BWCs is rising quickly. StorageCraft introduces StorageCraft for Law Enforcement, an easy to manage, flexible, and highly scalable video storage solution. Law enforcement agencies can start with 10 terabytes of storage and scale up to petabytes in the same cluster. They can add any number of drives, anytime and in any granularity, to meet their storage requirements. And, when they expand their available storage capacity, there is zero configuration and no application downtime.

For more information, visit www.storagecraft.com.

WLI WOMEN'S LEADERSHIP INSTITUTE

IACP's Women's Leadership Institute (WLI)

addresses the unique challenges and opportunities women face and helps them to succeed as they rise through leadership positions in public safety organizations. The course is open to men and women in sworn and non-sworn positions.

Women's Leadership Institute participants will:

- Further leadership skills and prepare for advanced leadership positions.
- Understand internal and external stakeholders and the impact of their individual differences.
- Learn the value of and how to have crucial conversations.
- Create a strategic career plan.
- Meet and learn from others to bring proven practices and strategies back to their organizations.
- Increase their professional network.

CURRENT OPPORTUNITIES

NASHVILLE, TENNESSEE, 2018
August 12-17

OTTAWA, CANADA, 2018
September 16-21

CHANDLER, ARIZONA, 2018
October 21-26

COST

$1,380. This includes course materials and select meals.
Early registration discounts available.

FOR MORE INFORMATION:

125 Years 1893 - 2018
IACP International Association of Chiefs of Police

WLITeam@theIACP.org • theIACP.org/WLI
800.THE.IACP

Today's Police Chiefs' Greatest Challenge

Accountability, Accountability, Accountability!

By Hajir Nuriddin, Captain (Ret.), Bakersfield, California, Police Department

In today's policing environment, maintaining trust is a constant internal and external challenge. Declining recruitment and retention efforts have created safety concerns for officers and communities, and, as a result of an exodus of experienced and qualified leaders, gaps in law enforcement leadership exist. High-profile incidents have created strategic uncertainty, and the constant political oversight and diminishing budgets have made it difficult, if not impossible, for chiefs to achieve their agencies' mission to protect and serve their communities. Many of these situations could easily merge to create a critical challenge or insurmountable situation for leaders to navigate. A "perfect storm" might, in fact, be looming for law enforcement.

In the midst of these myriad issues, the greatest challenge may be ensuring police accountability. With daily allegations of police misconduct (e.g., excessive force, assaults, and unfair treatment of community members) and the unfortunate realities of some of these accusations, there is a growing perception that police are incapable of holding themselves accountable. As chiefs continue to operate under intense scrutiny and oversight, they are acutely aware that they may be one incident away from being the next "breaking news" headline. The key to establishing accountability is developing an understanding and an effective strategy.

Police accountability can be defined as "a system of internal and external checks and balances aimed at ensuring" police personnel carry out their duties properly and holds them responsible should they fail to do so. Such a system is meant to uphold police integrity, deter misconduct, and restore or enhance public confidence in policing.[1]

The concept and application of police accountability, is ever expanding, and more complex than many imagine. Accountability is often demanded, to different degrees, by a variety of stakeholders—activists; news media; politicians; unions; citizen review boards; and, of course, community members. How does a chief balance the competing demands and expectations? How does a chief provide accountability to the broader environment? Does accountability mean enforcing discipline in response to the actions of officers, only to have decisions overturned by external review boards, arbitrators, or civil service commissions? Or does it mean supporting and standing by officers' actions regardless of external pressures? Has the scope and core meaning of police accountability been overextended? Is it unrealistic to believe this level of accountability is achievable? To answer these questions and find their way to better accountability practices, law enforcement leaders need to look at four key factors that affect accountability—leadership, trust, use of force and technology, and politics.

Four Key Factors Impacting Police Accountability

Authentic Leadership

Leadership is law enforcement's greatest tool to ensure police accountability. Chiefs and others in leadership roles must set the tone for their officers! They are responsible for providing guidance and support, modeling integrity, and holding officers accountable for their actions. Internal structures are not enough. Officers don't commit to policies, procedures, or processes—they commit to the causes and purposes advanced by great, authentic leaders.

> *"No one is compelled to choose the profession of a police officer, but having chosen it, everyone is obligated to live up to the high standards of its requirement."*[2]
>
> —President Calvin Coolidge

Community Trust

The community outcry and demand for accountability cannot (and should not) be ignored: "I just want the police to be held accountable"; "We just want the system of policing to be held accountable"; and "Police need to be held accountable the same way you would hold me accountable if I broke the law."[3]

In response to these concerns, law enforcement leaders must create opportunities to facilitate authentic problem-solving conversations with community stakeholders to develop models that address the specific concerns in their respective communities.

Use of Force and Technology

Use of force by law enforcement is probably one of the most prevalent contributors to the call for increased police accountability. Incidents are fueled by the 24/7 social media posts that go viral

within seconds. In an effort to counter this issue, chiefs are searching for methods and new technology (e.g., body-worn cameras, algorithms, and drones) to reduce future high-profile incidents.

The focus on systems, structures, and processes is important to demonstrate transparency to members of the community; however, training officers on "why" they serve and the origin of their power and authority may be part of the solution by developing self-accountability. Police officers solemnly swear to uphold the laws of their countries, yet most have never read their country's constitution or equivalent guiding document. Many officers are not aware that their power and authority is derived from the people through the social contract.[4] The social contract requires that those who accept the power and authority that comes with the position of police officer also accept the five standards of responsibility (fair access, public trust, safety and security, teamwork, fairness, and objectivity).[5]

Although there is no guarantee, training officers on self-accountability, coupled with "solid" effective supervision and transparent processes and systems, might be the solution to improving accountability across the profession.

> *"What I know is that body cameras are not the panacea. Body cameras will never replace dialogue or relationships.*
>
> *If we put all of our hope in a technology solution for a human problem, we will be disappointed."*[6]
>
> — Chief Will Johnson, Arlington, Texas

Politics

It is not uncommon, that when police chiefs discipline and hold officers accountable for misconduct or negative behaviors, their decisions are derailed by political intervention, sometimes resulting in the disciplinary actions being overturned. This often results in unfit officers continuing to deliver substandard police service. The continued service of unsuitable and unethical officers erodes trust, destroys internal and external organizational integrity, and undermines accountability efforts to members of the community

Historically, the early development of police departments meant the presence of political and economic corruption within the departments.[7]

> *Politicians ran precincts as small departments. This meant that the mission of the police was also the same mission of their local politicians.*[8]

Since the early 1900s, police organizations have made tremendous ethical strides and developments; however, chiefs and other law enforcement executives still struggle to retain full responsibility and authority to effectively lead and hold their personnel accountable without political interference.

Ultimately, chiefs in conflict with unethical governing politicians must have the moral courage to remain true to their core principles and values, which may entail stepping down or being forced out.

> *"Since 2006, the nation's largest police departments have fired at least 1,881 officers for misconduct that betrayed the public's trust, from cheating on overtime to unjustified shootings… departments have been forced to reinstate more than 450 officers after appeals required by union contracts."*[9]
>
> —Washington Post

Conclusion

Stakeholders have an expectation of police accountability, and law enforcement leaders have the responsibility to deliver it. Ensuring an appropriate level of accountability may be challenging, chaotic, and daunting, but it nonetheless remains every chief's duty to hold officers accountable and uphold the sacred trust of policing. ❖

Notes:

[1]United Nations Office on Drugs and Crime, *Handbook on Police Accountability, Oversight and Integrity*, Criminal Justice Handbook Series (New York, NY: United Nations, 2011), 9, http://www.unodc.org/documents/justice-and-prison-reform/crimeprevention/Police_Accountability_Oversight_and_Integrity_10-57991_Ebook.pdf.

[2]G.B. Jones, "Law Enforcement: Do It J-U-S-T-I-C-E," Notable Speeches, *FBI Law Enforcement Bulletin*, September 1, 2012, https://leb.fbi.gov/bulletin-highlights/notable-speeches/notable-speech-law-enforcement-do-it-j-u-s-t-i-c-e.

[3]John Oliver, "Police Accountability," *Last Week Tonight*, October 2, 2017, https://www.youtube.com/watch?v=zaD84DTGULo.

[4]John Locke, *Two Treatises of Government: A Critical Edition with an Introduction and Apparatus Criticus*, ed. Peter Laslett (Cambridge, England: Cambridge University Press, 1970).

[5] Howard S. Cohen. and Michael Feldberg, *Power and Restraint: The Moral Dimension of Police Work* (Westport, CT: Praeger Publishers, 1991), 39–66.

[6]Ellen Meyers, "Arlington Police Chief: Body Cameras Aren't Effective in Building Trust with Public," *Dallas News*, July 11, 2016, https://www.dallasnews.com/news/dallas-ambush/2016/07/11/arlington-police-chief-consider-body-cameras-effective-building-community-trust.

[7]Roy Roberg et al., *Police & Society*, 6th ed., Chapter 2 (New York, NY: Oxford University Press, 2014).

[8]Community Policing.com "History of Policing," http://www.communitypolicing.com/history-of-policing.

[9]Kimbriell Kelly, Wesley Lowery, and Steven Rich, "Fired/Rehired," *Washington Post*, August 3, 2017, https://www.washingtonpost.com/graphics/2017/investigations/police-fired-rehired.

Captain Nuriddin was one of the many great presenters at IACP 2017.

Want to learn more about leadership and law enforcement topics? Visit www.theIACPconference.org to register for IACP 2018 and to see the great speakers and topics scheduled for this year's event!

JOIN US!

IACP 2018
October 6–9, 2018
Orange County Convention Center
Orlando, Florida
theIACPconference.org

New Technology and Funding Opportunities

By Domingo Herraiz, Director, Programs, IACP

For many years, public safety's use of radio spectra within the United States existed in disparate bands allocated by the Federal Communications Commission and the National Telecommunications Information Administration (NTIA). This caused various communication problems for public safety entities, and one of the key findings of the 9/11 Commission was the need for the creation of a National Public Safety Broadband Network (NPSBN).[1] Thus, for many years following 9/11, various police, fire, and EMS organizations came together to promote the benefits of a stand-alone, dedicated public safety broadband network with the necessary continuous spectrum. After years of negotiation, the U.S. Congress finally gave public safety the dedicated spectrum the field needed by establishing the First Responder Network Authority (FirstNet) to provide U.S. emergency responders with the first nationwide, broadband network dedicated to public safety.

Last year, FirstNet awarded a contract to deploy the first dedicated broadband network for U.S. public safety, and the fall of 2017 saw all 50 states, all U.S. territories, and the District of Columbia opting into the network. This was a monumental achievement that would not have been possible without the unwavering support from public safety. End-to-end encryption, security monitoring, system reliability, and local control are all possible after more than a decade of dedicated work by IACP members, who played a key role in ensuring mission critical requirements were taken into consideration.

It is time for law enforcement to begin planning for the use of this critical infrastructure. Emergency communications is just one of the many technological challenges that have taken place in recent years—mobile devices, next generation 911, intelligence and information sharing environments, rapid DNA, digital evidence, and other technological advances will drive law enforcement for many years to come, assisting the field with crime prevention and investigation.

When thinking about these various public safety technological advances for departments and the communities they serve, agencies must also consider funding opportunities that might exist. Various federal grants can provide financial assistance for agencies considering new technologies to create safer communities.

U.S. Grant Funding Opportunities

For many years, the U.S. government has provided funding for state, local, territorial, and tribal (SLTT) law enforcement to procure services and equipment. With the advent of the Department of Justice's Law Enforcement Assistance Administration (LEAA) in 1968, direct funding to law enforcement agencies began to flow. The LEAA's intent was to provide funding to state and local governments for educational programs, research, criminal justice planning, and local crime initiatives. In 1994, the Office of Community Oriented Policing Services (COPS Office) was created, providing significant resources for law enforcement's expanded efforts in community policing, which included funding for police hiring, programming, and equipment. Additionally, from 1996 to 2006, Congress funded the Local Law Enforcement Block Grant (LLEBG) program to support public safety and crime prevention efforts. In 2006, the LLEBG program was merged into the Edward Byrne Memorial Grants Program to create the Edward Byrne Memorial Justice Assistance Grants Program (Byrne JAG) to focus more specifically on criminal justice personnel, training, equipment, and supplies. Today, this program passes funding directly to the largest jurisdictions and through state criminal justice agencies to smaller local government entities. The Byrne JAG program and the COPS Office's grant programs continue to provide local law enforcement with needed resources.

The U.S. Department of Homeland Security, created in 2002, is another source of funding for SLTT law enforcement through the Federal Emergency Management Agency. These funds are used for preparedness programs to enhance the capacity of SLTT emergency responders to prevent, respond to, and recover from a weapons of mass destruction terrorism incident.

Just like the creation of these past grant programs, one can also imagine the creation of future funding programs to assist law enforcement with purchases of new technology. For example, in 2015, the U.S. Congress and the Department of Justice created a funding opportunity for jurisdictions interested in implementing a body-worn camera strategy. It is plausible that, in the future, law enforcement could see similar additional funding streams for specialized equipment that could also advance the profession, such as LTE devices that would run on the FirstNet broadband network.

Focus on Grant Writing

The first step for an SLTT agency seeking to secure grant funding is to know what funds might be available. Registering for federal funding announcements with Grants.gov is a starting point for being aware of these opportunities. Once potential funding opportunities are identified, the next step is to recognize that the technology the funding will provide for is only a means to an end. The grant application or proposal must focus on the overarching initiative to reduce crime in the community and keep officers safe. Agencies should focus on the problem they are trying to address, what they are ultimately trying to accomplish, how this technology will make a difference, and how the solution will improve community safety.

Grant programs will ask applicants to tell the story of what the issues have been in the past and how what the agency is proposing will make a difference in building safer communities and safer officers. Agencies will need to provide a statement of the problem, the project design, the implementation strategy, the capabilities and competencies of the agency (including any past grants and their management), a budget with a narrative as to why the items are needed, and a timeline of the project's anticipated accomplishments. These elements can be prepared ahead of any grant announcement, making grant applications easier to compile when a funding opportunity is released.

Future Perspective: Technology and Funding

Over the last 10 years, the world has seen an explosion in personal technologies, and a similar growth is beginning to happen within the law enforcement profession. It is no surprise that technology plays a significant role in law enforcement profession and strategies to help keep communities and officers safe. Over the last several years, automated license plate readers; unmanned aircraft systems; real-time crime centers; body-worn cameras; autonomous vehicles; and, now, FirstNet devices have been among the technologies that affect law enforcement. With the advent of artificial intelligence and new technology opportunities, who knows what the next emerging technology will be? What is known is that opportunities in technological advancement for law enforcement will be endless, and law enforcement agencies must be prepared with implementation and funding development strategies. ❖

Note:

[1]National Commission on Terrorist Attacks Upon the United States, *The 9-11 Commission Report*, 2004.

WHERE DO YOU TURN

WHEN YOU NEED ANSWERS

ABOUT POLICY AND BEST PRACTICES?

We have the information you are looking for.
IACP Net,℠ the business resource for law enforcement, makes it easy to access the information and best practices you need to serve your department and your community.

STRATEGIES
Develop your policing strategies with case studies and best practices.

RESOURCES
Leverage vetted information and resources.

POLICIES
Update policies and forms with ready-to-use samples including model policies.

SHARING
Exchange information, best practices, and lessons learned with other agencies.

Learn more and subscribe to IACP Net by visiting
CommandAnswers.com
or call 800.227.9640.

@IACPNet

IACPnet

125 Years
1893 - 2018
IACP
International Association of Chiefs of Police

Crash Reporting Centers: Moving Crash Reporting Away from the Roadway

By Howard B. Hall, Chief, Roanoke County, Virginia, Police Department

Law enforcement leaders face a never-ending challenge to provide exceptional service while controlling costs. The lack of new resources to meet continually increasing demands requires that traditional responses be reexamined. Assigning police officers to investigate and report property damage–only (PDO) motor vehicle crashes is an example of an area where police time can be saved and reassigned to higher priority needs. The use of crash reporting centers (CRCs) is proving to be a viable alternative to the traditional response.

Like most agencies, police in the Roanoke Valley, Virginia, conformed to the traditional practice that requires a police officer to respond to the scene of a PDO crash to conduct what is often a perfunctory investigation and prepare a state-mandated report, which is then submitted to a supervisor for review. This labor-intensive activity frequently results in lengthy traffic disruptions; however, the data gathered are critical to the development of effective traffic safety programs. For this reason, alternative responses that reduce officer time must preserve the collection of crash-related data.

Through participation in various IACP and Virginia Association of Police Chiefs events, Roanoke Valley law enforcement leaders learned of a program designed to reduce the amount of time an officer spends engaged in handling a PDO collision. The use of CRCs is a highly successful program that has been in place for more than 20 years in Canada. A CRC provides a way to move the reporting of certain crashes from the roadside to a safe, comfortable facility where civilian counselors facilitate the crash report process.

Canadian CRCs have led to a variety of benefits for both law enforcement and motorists. Police officer time is saved by transferring reporting responsibility to the centers. With the crash reporting process moved from the roadside to the centers, roadway clearance is quicker, thus increasing the safety of first responders and motorists, as well as reducing the congestion that often leads to secondary crashes. Off-scene reporting is convenient to motorists, who are allowed 48 hours to report to the center, and this program is highly acclaimed by the Canadian motoring public.

The Canadian program was fashioned in a partnership between Toronto Metropolitan Police Service (TMPS) and an industry provider. This allowed TMPS to eliminate the vast majority of police time typically dedicated to reporting PDO crashes, as that time commitment was shifted from TMPS personnel to the external provider's employees at the CRCs. The centers' staff handle the complete process of crash reporting, and involved motorists either drive or have their damaged vehicle towed to the CRC. A CRC staff member ("counselor") photographs the damaged area of a vehicle and affixes a security sticker noting that the damage has been reported to the police, which helps to deter insurance fraud. CRC personnel complete a government-mandated traffic collision report, secure written statements from drivers, and use the accounts from the reporting parties to provide a computer-supported crash diagram. CRC collision reports are reviewed by the designated member of the police agency before reports are entered into the agency's records management system and provincial traffic records system.

Roanoke Valley police agencies invited representatives from TMPS's industry partner, Accident Support Services, Inc., to make a presentation before interested police and government leaders. This resulted in careful planning that led the cities of Roanoke and Salem and the county of Roanoke to conduct a one-year pilot project. The Roanoke Valley Collision Reporting Center (RVCRC) opened in September 2016, becoming the first operation of its kind in the United States.

As with any new program, start-up requires modifications to achieve optimal results. A CRC is not a "cookie-cutter" solution, as each jurisdiction and police agency has it owns requirements for crash reporting. Each center is developed to meet the needs of the involved police agency. The standard Canadian method for reporting, reviewing, and approving reports was implemented in the RVCRC with some modifications, and officers from participating agencies respond to the scene of most PDO collisions to determine if police intervention beyond assisting the motorists is required.

Officers continue to handle PDO crashes if any of the following conditions are present:

- driver impairment
- failure to stop, render aid, and self-identify
- criminal conduct other than a traffic infraction identified as a causative factor
- commercial vehicle
- transportation of hazardous material
- government-owned or government-operated vehicle

Motorists involved in PDO crashes that do not have any of the previously listed factors are referred to the CRC. In these cases, each involved motorist is provided with an agency-approved

Motorists involved in simple property damage–only collisions are referred to the CRC for post-collision services like reporting and insurance claims.

brochure that facilitates the capturing of information about the others involved, provides the location of the RVCRC, and explains how to file a police report.

Experience suggests that as the police and residents of Roanoke Valley become more fully informed about the CRC, public safety dispatchers will become accustomed to referring motorists directly to the CRC when PDO crash calls come in.

In lieu of towing vehicles to the CRC, which involves additional costs, police personnel worked with their industry partner to develop an application using tablet computers to photograph disabled vehicles at crash scenes. Police photographs are automatically uploaded to the RVCRC server for inclusion with the collision report. Drivable vehicles are taken to the RVCRC where counselors take photographs.

The RVCRC is provided at zero cost to the agencies, governments, or citizens served. All costs of creating and operating a CRC are paid by insurers. By using CRC-generated reports, insurers have quicker access to collision data, allowing for faster claim settlement, which is a direct cost savings. Insurance fraud control is enhanced by the CRC's practice of taking photographs and affixing a "police reported" sticker, thus further reducing cost to insurers.

The Roanoke region's pilot program was evaluated after one year and determined by participants to be a success. It achieved the goal of relieving police officers of the time-consuming task of preparing a police report for PDO crashes, therefore freeing them to perform other duties and tasks. The quality of reports generated by the CRC is equal or better than what was available before, and they are completed in a timely manner. Clearly the most meaningful proof of success is the citizen surveys that rank the RVCRC with more than a 98 percent customer satisfaction rating. For these reasons, the three governments extended their agreements with the CRC provider for five additional years.

Although the CRC concept is still new to the United States, the experience in Roanoke is proving that this model offers benefits to police agencies, motorists, and insurance companies. Interest from other parts of the United States is increasing, and additional centers are likely to open later this year. In the long term, the use of CRCs may become the new standard for reporting PDO crashes worldwide. ❖

"Police Reported" stickers for damaged vehicles photographed at the CRC.

FURTHER READING

Access past Traffic Safety Initiative columns or traffic safety–related articles at Police Chief Online by selecting "Traffic Safety" from the Topics dropdown menu or "Traffic Safety Initiatives" from the Columns dropdown menu. You can also search for specific articles, authors, or topics using the site's search feature.

Visit Police Chief Online at www.policechiefmagazine.org.

Please Join Us

IACP Annual Banquet

featuring the presentation of our

2018 IACP LEADERSHIP AWARDS

and the

SWEARING-IN OF THE IACP PRESIDENT AND EXECUTIVE BOARD

Tuesday • October 9 • 6:00 pm – 11:00 pm

Valencia Ballroom, Level 4

Orange County Convention Center — West Building

Purchase tickets online at **theIACPconference.org**

IACP 2018 October 6–9 Orlando FLORIDA
International Association of Chiefs of Police

IACP 23rd Annual Training Conference on Drugs, Alcohol, and Impaired Driving

By Chuck Hayes, Project Manager, IACP

The International Association of Chiefs of Police (IACP), working in partnership with the National Highway Traffic Safety Administration (NHTSA), and various state highway safety offices, continues to provide one of the premier impaired driving training conferences in the world. The 2017 IACP Annual Training Conference on Drugs, Alcohol, and Impaired Driving (DAID Conference) was held in National Harbor, Maryland, and attracted close to 1,000 attendees.

The DAID Conference provides drug recognition experts (DREs), police officers, toxicologists, prosecutors, and other traffic safety professionals with a forum in which to share information, learn about best practices, and find out about efforts to deter impaired driving and make the roadways safer. Technology and practices are constantly evolving, and the DAID Conference provides consistent training, professional development, and information for DREs and other highway safety professionals on a broad array of new and emerging impaired driving issues.

The 2018 DAID Conference will be held August 13–15 at the Gaylord Opryland Resort & Convention Center in Nashville, Tennessee. The annual DRE State Coordinators meeting will take place the day prior to the conference on August 12. At the 2018 DAID Conference, a mix of plenary sessions and concurrent workshops will keep attendees up-to-date and informed on a range of topics, including the implications of central nervous depressants and their effects on driving, as well as other relevant issues. In addition, conference attendees will have access to the following:

Premier training. Whether a DRE, highway safety advocate, law enforcement officer, prosecutor, toxicologist, or a private or nonprofit highway safety program provider, conference attendees will be provided with exceptional, informative training, including workshops focusing on many of the "hot topics" on impairment-causing drugs and impaired driving.

Affordable rates. Government-rate lodging and a budget-friendly registration fee are available, making the conference one of the most affordable international training events.

Knowledgeable speakers. Plenary sessions and workshops will feature knowledgeable subject matter experts from the areas of impaired driving, drug impairment, drug toxicology, and the prosecution of challenging impaired driving cases.

Networking opportunities. Formal and informal networking opportunities through conference workshops and other activities will be available.

State-of-the-art technology. Numerous companies, organizations, and government agencies will exhibit the latest impaired driving products, programs, and publications.

Professional development. Learning about new and proven strategies will help improve attendees' productivity and allow the sharing of important impaired driving information.

Return on investment. Attendees can expect to return from the conference with new ideas, best practices, and resources that can be used right away to help benefit their agencies and their communities.

DRE recertification. For DREs, the conference will fulfill the required eight hours of recertification training and provide updated and relevant information that will benefit their agencies, fellow DREs, and communities.

Another important activity that occurs each year at the DAID Conference is the recognition of individuals who have made notable contributions to the Drug Evaluation and Classification (DEC) Program. Special recognitions are made in the following areas:

DRE Emeritus: Available only to formerly certified DREs who have served the purposes of the DEC Program honorably and with the highest integrity and who are no longer eligible or capable of maintaining DRE certification (such as through retirement or promotion to an executive position).

DRE Ambassador: Available to an individual who has contributed significantly to the DEC Program, but who is not and has not been a certified DRE.

Karen Tarney-Bookstaff DRE-of-the-Year: Presented annually by the IACP DRE Section to a certified DRE who demonstrated outstanding contribution to the DEC Program for the previous calendar year.

Information regarding these three exclusive recognitions, granted only by the IACP DRE Section, can be accessed at the DRE Section webpage (www.theIACP.org/Drug-Recognition-Expert-Section).

IACP Drug Recognition Expert Section

In 1992, the IACP governing body approved the creation of the IACP Drug Recognition Expert (DRE) Section. The primary purposes

Drug Recognition Experts—Making an Impact During Impaired Driving Crackdowns

By Kyle Clark, Project Manager, and Chuck Hayes, Project Manager, IACP

Each year the U.S. Department of Transportation's National Highway Traffic Safety Administration (NHTSA) holds U.S.-wide impaired driving enforcement crackdown campaigns aimed at reducing impaired driving crashes and related deaths and injuries on roadways.[1]

An important, but often underutilized component of each campaign is the proactive and effective use of drug recognition experts (DREs), which are police officers specially trained to identify and apprehend drivers suspected of being under the influence of alcohol and other drugs.[2] Utilizing their drug-impairment detection skills, DREs can play an integral role in addressing impaired driving, particularly during impaired driving crackdown campaigns.

The IACP and NHTSA continue to encourage law enforcement agencies to utilize DREs during each crackdown campaign. According to IACP DRE records, there are now more than 8,000 DREs in the United States.[3] These officers can be major contributors in special emphasis patrols, DUI checkpoints, or DUI processing locations to screen suspected drug-impaired drivers and to conduct drug evaluations.

In 2017, two high-profile impaired driving crackdown campaigns were held during the Labor Day holiday period and the December to New Year holiday period. Forty-two DRE state coordinators provided DRE enforcement data during the Labor Day campaign period. DREs from those 42 states conducted 7,404 DUI arrests, made 1,124 driving under the influence of drugs (DUID) arrests, and conducted 1,304 DRE drug influence evaluations. The DREs also participated in 550 DUI sobriety checkpoint operations and were involved in 1,712 DUI emphasis patrols. In addition to their impaired driving enforcement activities, the DREs also made 5,464 drug arrests during the campaign period.

During the December to New Year campaign period, held December 12, 2017, through January 1, 2018, DREs from the reporting states accounted for 6,569 DUI arrests and 1,294 DUID arrests and conducted 1,163 drug influence evaluations. The DREs also participated in 340 sobriety checkpoints and were involved in more than 1,500 impaired driving emphasis patrols and special events. They also made 2,291 drug arrests during the campaign period. Three of the more active states during the December to New Year campaign were California, where DREs made 276 DUID arrests; Arizona, with 217 DUID arrests; and New York, with 109 DUID arrests.

In addition to the impressive enforcement totals, DREs were involved in numerous other enforcement activities, which included the following successes:

- **Colorado:** Two DRE-related DUID investigations resulted in the seizure of guns, money, and methamphetamine, and felony DUI charges resulting from an impaired driver crash with a police vehicle.
- **Idaho:** A DRE was responsible for conducting a drug trafficking investigation that resulted in the seizure of 1.2 pounds of methamphetamine.
- **Maryland:** A DRE who responded to a drug overdose call performed CPR and resuscitated the victim. A warrants check revealed the subject was wanted for armed kidnapping and manslaughter.
- **Oregon:** A DRE assisted his agency with investigations leading to the seizure of over four ounces of heroin and other multiple methamphetamine seizures. Another DRE, who is also a narcotics detection K9 handler, deployed his canine, resulting in the seizure of two ounces of heroin and 35 grams of methamphetamine. Yet another DRE arrested a suspect for DUID and discovered the suspect was also involved with child pornography, leading to numerous other criminal charges being filed.

This information, compiled from the DRE state coordinators, demonstrates the importance and effectiveness of having DRE-trained officers on patrol and involved in impaired driving crackdown campaigns.

Notes:

[1]National Highway Traffic Safety Administration, "Drug-Impaired Driving," https://www.nhtsa.gov/risky-driving/drug-impaired-driving.

[2]IACP, International Drug Evaluation & Classification Program, "Drug Recognition Experts (DRE)," http://www.decp.org/drug-recognition-experts-dre.

[3]IACP DRE database, February 1, 2018.

of the section are to serve as a coordinating body among the various DRE associations or chapters within states, to serve as a resource for officers, and to respond to the views and needs of the membership. Drug recognition continues to be an excellent tool in identifying and prosecuting drug-impaired drivers. Professional interest in the Drug Evaluation and Classification (DEC) Program and procedures has grown from impaired driving enforcement to include workplace drug impairment evaluation, juvenile justice, corrections, and other fields. The IACP DRE Section provides an opportunity for those professionals already associated with drug recognition to share common management, training, administrative, and practicing concerns. Recertification training, continuing and advanced education, creative teaching techniques for instructors, certification problems and solutions, and the development and sharing of databases are some of the issues considered by the DRE Section. The section provides DREs, the practitioners of drug influence recognition, and program coordinators with an ongoing forum for a discussion of needs and concerns through membership in the DRE Section. ❖

To learn more about the DAID Conference, including registration and lodging information, visit the 2018 DAID Conference webpage at www.theIACP.org/DAID Conference.

To learn more about the IACP DRE Section, including how to join the section, visit the IACP DRE Section page at www.theIACP.org/Drug-Recognition-Expert-Section.

WATCH

Find out what past DAID Conference attendees have found valuable by watching the video at www.theIACP.org/DAIDconference, featuring the top five event take-aways.

INDEX TO ADVERTISERS

The advertisers in this issue can help equip your department with the most efficient tools available today!

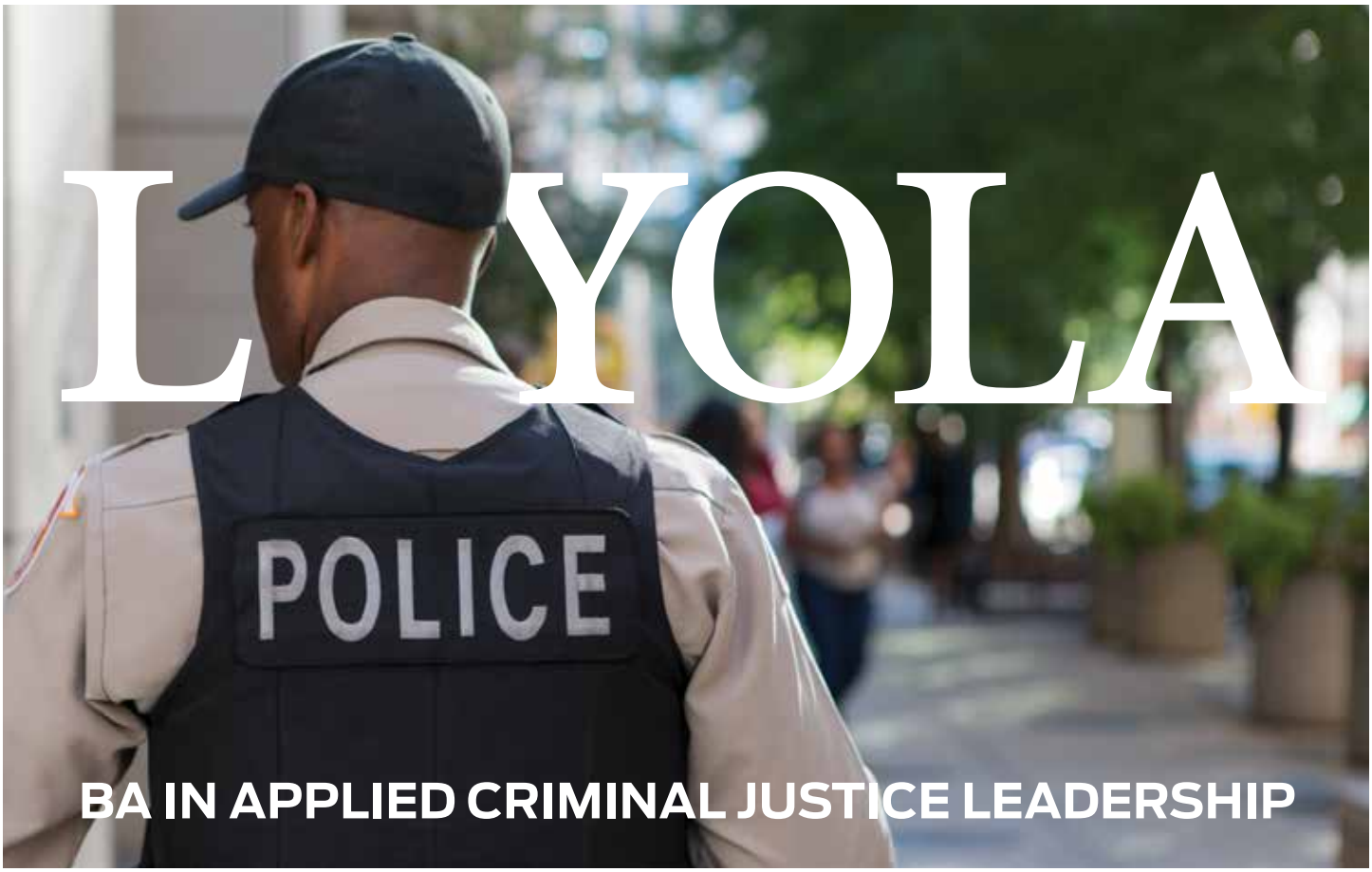
Always mention the *Police Chief* when contacting our advertisers.

	Page #
2018 IACP/Target Police Officer of the Year 800.THE.IACP www.theiacp.org/poy	63
Accident Support Services International 877.895.9111 www.accsupport.com	34–37
ASIS International 703.519.6200 www.asisonline.org/pcm	2
AT&T 571.665.6100 www.firstnet.com	16–17
ATF Police Officer's Guide to Recovered Firearms 800.THE.IACP www.theiacp.org/firearmsapp	40
Axon (Formerly TASER) 800.978.2737 www.axon.com/fleet2	3
Envisage Technologies 888.313.8324 http://info.acadis.com/ultimate	11
First-Line Leadership Training 800.THE.IACP www.theiacp.org/first-line-leadership	71
IACP 2018 Annual Banquet 800.THE.IACP www.theiacpconference.org	79
IACP 2018 Annual Conference and Exposition 800.THE.IACP www.theiacpconference.org	53
IACP 2018 Housing 800.THE.IACP www.theiacpconference.org	56
IACP 2018 Registration 800.THE.IACP www.theiacpconference.org	55
IACP Drugs, Alcohol, and Impaired Driving Conference 800.THE.IACP www.theiacp.org/daidconference	9
IACP Member-to-Member Drive 800.THE.IACP www.theiacp.org/membership	64–65
IACP Net 800.227.9640 http://iacpnet.com	77
IACPreferred (Member Benefits) 800.THE.IACP www.theiacp.org/welcome-to-iacpreferrred	33, 68
IAPro 800.620.8504 www.iapro.com	5
L3 Mobile-Vision 800.336.8475 www.bwx100.com	13
Laser Labs, Inc. 800.452.2344 www.laser-labs.com	7
Leadership in Policing Training 800.THE.IACP www.theiacp.org/lpo	71
LexisNexis Coplogic Solutions 877.719.8806 www.lexisnexis.com/coplogic	22–23
Loyola University Chicago 773.508.3396 www.luc.edu/iacp	83
Molex, LLC 716.566.2728 www.sensorcon.com	21
Northwestern University Center for Public Safety 800.323.4011 http://nucps.northwestern.edu	41
Planning, Designing, and Constructing Police Facilities Course 800.THE.IACP www.theiacp.org/planning-designing-and-constructing-police-facilities	21
Policestickers.com 508.982.1555 www.policestickers.com	5
Reeves Company, Inc. 800.452.1161 www.reevesnamepins.com	27
Salsbury Industries 800.562.5377 www.lockers.com	Exsert
Sirchie 800.356.7311 www.sirchie.com	49
Smith & Wesson 800.331.0852 www.smith-wesson.com	15
Southern Police Institute 502.852.6561 www.spiaa.org	59
Super Seer Corporation 800.645.1285 www.superseer.com	47
Total Recall Corporation 800.659.7793 www.convergint.com/crimeeye-video	84
Women's Leadership Institute 800.THE.IACP www.theiacp.org/wli	73

*Please contact **The Townsend Group, Inc. at 301-215-6710** if you are interested in or have questions about advertising in* Police Chief.

The IACP does not recommend, endorse, or accept responsibility for the proper performance of any product advertised in these pages.

SCHOOL OF CONTINUING AND PROFESSIONAL STUDIES



FASTRACK YOUR DEGREE
ONLINE • EVENINGS • WEEKENDS

You're invited to apply for Loyola's fully online program aimed at developing leadership skills such as critical thinking and ethical reasoning in current criminal justice professionals.

Loyola's online bachelor's degree programs have been recognized by *U.S. News and World Report*.

RANKED	TOP
#1	15
IN ILLINOIS	IN THE NATION

Applications are accepted on a rolling basis.
Get started at **LUC.edu/IACP**.

LOYOLA UNIVERSITY CHICAGO
1870
AD • MAJOREM • DEI • GLORIAM

Preparing people to lead extraordinary lives

Looking to Deter Crime and Improve Situational Awareness? The CrimeEye® RD-2 Can Help.

CrimeEye RD-2

- Self-contained and lightweight turnkey public safety video system
- Functions independently or can integrate into a citywide network
- Requires virtually no tools and can be set up in a quick, single-person installation
- Streams high-quality video within minutes of installation
- Patented enclosure

To learn more, visit
www.convergint.com/CrimeEye-video

NOW AVAILABLE WITH GUNSHOT DETECTION

TRANSPORT MODE

Genetec™

TOTAL RECALL CORPORATION
A Convergint Technologies Company
Phone: 800-659-7793